PERSEREC

Technical Report 03-2
November 2002

Model for a Future Defense Personnel Security System

Eric L. Lang
Katherine L. Herbig
TRW Systems

Research Conducted by
Defense Personnel Security Research Center

Technical Report 03-2 **November 2002**

Model for a Future Defense Personnel Security System

Eric L. Lang
Katherine L. Herbig
TRW Systems

Released by
James A. Riedel
Director

Defense Personnel Security Research Center
99 Pacific Street, Suite 455-E
Monterey, CA 93940-2497

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* November 2002	2. REPORT TYPE Technical	3. DATES COVERED *(From – To)* September 2000 to October 2002

4. TITLE AND SUBTITLE Model for a Future Defense Personnel Security System	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Eric L. Lang Katherine L. Herbig	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	8. PERFORMING ORGANIZATION REPORT NUMBER PERSEREC TR 03-2
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Defense Personnel Security Research Center 99 Pacific Street, Suite 455-E Monterey, CA 93940-2497	10. SPONSORING/MONITOR'S ACRONYM(S) 11. SPONSORING/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The "Options project" considered published reports and evaluations of DoD's personnel security program, relevant program initiatives, strategic goals, organizational principles that have been shown to enhance effectiveness, the role of information technology, personnel security practices outside of DoD, and insights from interviews of personnel security experts in order to design a more coherent and effective personnel security *system*. This approach yielded a model with five organizational elements, three of which: Requirements and Adjudication Management Programs (RAMPs), the Defense Investigation Technology and Tracking Office (DITTO), and the Personnel Security Oversight Committee (PSOC), are novel organizational entities. The report describes organizational roles in the proposed "RAMPs/DITTO model," and recommends that an Acting PSOC be established to manage implementation.

15. SUBJECT TERMS

Personnel Security, Personnel Security Requirements, Business Process Re-engineering, Information Systems, Organization Management, Business Systems, Investigative Providers, Central Adjudication Facilities

16. SECURITY CLASSIFICATION OF: Unclassified			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF REPONSIBLE PERSON James A. Riedel, Director
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER *(Include area code)* 831-657-3000

Preface

This report presents the results of a study entitled *Options for Future Defense Personnel Security Systems*, tasked by the Deputy Assistant Secretary of Defense for Security and Information Operations (S&IO), Command, Control, Communications, and Intelligence (C3I). The goal of the Options project was to consider past and present initiatives, current strengths and problems, and future challenges in a "big picture" study to inform the design of a better, more coherent, personnel security system.

The Options approach focused on designing an end-to-end personnel security system that increases coordination regarding management, authority, resources, and accountability. We addressed organizational roles in four critical areas: [1] requirements for investigations and periodic reviews, [2] investigations, [3] adjudications, and [4] information technology. We believe that the resulting model combines current system strengths, recent innovations such as the Joint Personnel Adjudication System (JPAS) and the Automated Continuing Evaluation System (ACES), broader and more effective use of information technology, and coordinated operational oversight to best serve DoD's needs in the coming decade and beyond.

James A. Riedel
Director

Acknowledgements

The authors appreciate the time and insights provided by many individuals who commented on early drafts of the Options model and briefings. Staff at the following organizations were particularly helpful: Army CAF, Navy CAF, Air Force CAF, Washington Headquarters Service, Defense Security Service, Office of Personnel Management, Security and Information Operations (OASD/C3I/S&IO), TRW Systems Fairfax office, and the Aerospace Industries Association.

Executive Summary

This report responds to a tasking by the Deputy Assistant Secretary of Defense for Security and Information Operations, Command, Control, Communications, and Intelligence (DASD [S&IO/C3I]) to consider past initiatives, current problems, and future challenges in a "big picture" study of the DoD personnel security program. The task required project staff to address the main components of the program: requirements for background investigations and periodic reviews, investigative processes, adjudicative processes, and supporting information technologies, and to go beyond a patch-on-patch approach of responding to problems.

The resultant project, entitled *Options for Future Defense Personnel Security Systems* (the "Options project"), considered published reports and evaluations of DoD's personnel security program, relevant program initiatives (such as the Joint Personnel Adjudication System), strategic goals, organizational principles that have been shown to enhance effectiveness, the role of information technology, personnel security practices outside of DoD, and insights from interviews and briefings of personnel security experts in order to design a more coherent and effective personnel security *system*. This approach yielded a model with five organizational elements, three of which, Requirements and Adjudication Management Programs (RAMPs), the Defense Investigation Technology and Tracking Office (DITTO), and the Personnel Security Oversight Committee (PSOC), are new organizational entities. Eight RAMPs are proposed: Army, Navy, Air Force, DIA, NSA, JCS, WHS, and industry.

The report describes organizational roles in the proposed "RAMPs/DITTO model," offers several suggestions for operational improvements, and illustrates how the anticipated system would perform in response to an unforeseen surge in personnel security requirements. Organizational functions and features addressed in this report include the following.

RAMPs

1. Managing PSI requirements estimation, including out years, through interactions with commands and/or organizational liaisons.
2. Managing the requirements budget and ongoing rate of utilization for the organization(s) it serves.[1]
3. Setting processing priorities for personnel requirements within the organization(s) it serves.
4. Adjudicating clearances by means of an internal adjudication facility.
5. Assigning adjudicators to PSI cases during investigation—the *Case Team* approach.
6. Acting as the single point of contact and help desk for the organization(s) it serves.

[1] For WHS, which adjudicates access determinations for the White House and several Defense agencies, the WHS RAMP would not control the requirements budget for the components it represents but would serve as a requirements coordination, monitoring, and processing center.

DITTO

1. Routing cases from the field, through the appropriate RAMP, to the assigned PSI provider (DSS or OPM).
2. Collecting data on DoD personnel security system operations, developing metrics and statistics, and generating status reports.
3. Serving as the POC for the RAMPs, PSI providers, and OSD for monitoring categories of cases, issuing early warnings, and conducting "what if" analyses.
4. Serving as the system administrator and life-cycle resource planner for the complete IT system.
5. Managing system flexibility to meet competing demands across RAMPs or between PSI providers.

PSI Providers

1. Two PSI providers (such as DSS and OPM) to enhance system flexibility and reduce the risk of system failure.
2. Each PSI provider has a guaranteed base workload, reviewed semiannually by the PSOC.
3. Each RAMP uses "fee for service" to pay for the provision of PSIs.
4. PSI providers address inquiries from RAMPs rather than directly from requesters in the field.
5. Investigators may work with adjudicators as a case team during the course of a PSI.

PSOC

1. Include representatives of the principal stakeholders, at a level sufficient to oversee Directors of the RAMPs, DITTO, and PSI providers.
2. Oversee DoD personnel security policy and operations.
3. Include a technical subcommittee as support for assessing and implementing technical solutions.

Summary of Benefits

In terms of expected improvements over the current personnel security program, the RAMPs/DITTO model should yield multiple benefits, such as:

- Increased ability for the military services, DoD agencies, and industry to predict personnel security requirements and to manage the process.
- Greater work efficiency through improved data and document transfers, file access, and integration of related databases.
- Improved management of information systems, technical support, and technology life-cycle planning.
- Improved ability to assess, report, and predict performance and resource utilization for individual organizations and the overall system.
- Improved system-wide operational oversight and program management.

Recommendation

An “Acting Personnel Security Oversight Committee” (APSOC) comprised of representatives of DoD components should be established to manage the process of reviewing and implementing changes suggested by this report. The APSOC should be chaired by an SES-level staff member of C3I/S&IO. Tasks for the APSOC should include:

1. Circulating the RAMPs/DITTO report for coordination and comment to appropriate managers at the Army, Navy, AF, DIA, NSA, JCS, WHS, and AIA/industry.
2. Developing a Statement of Work (SOW) to be used in soliciting proposals for one or two Independent Planning Studies (IPS) on creating DITTO. At a minimum, the IPS SOW should stipulate that each IPS would produce:
    a. a detailed architectural description (C4ISR compliant),
    b. cost and schedule estimates for full system development, including Costs As an Independent Variable,
    c. a documented Analysis of Alternatives, including considerations for using parts or all of CCMS,
    d. a transition plan for moving from current DoD systems to the proposed system, and
    e. a recommended acquisition approach, including attention to Clinger-Cohen Act and MAISARC/MAISAP requirements.
3. Securing funding for one or two IPSs on creating DITTO.
4. Overseeing the development of predictive models of personnel security requirements, including:
    a. tasking the Army and Navy to pursue the development of personnel security requirements models that capitalize on current achievements and knowledge gained through the Air Force model-building effort, and
    b. coordinating with efforts at DSS’s Central Requirements Office (CRO), which has conducted a survey of defense contractors to explore requirements prediction methods for industry.
5. Finalizing and submitting the Draft DoD Strategic Plan for Personnel Security to the ASD C3I for authorization and promulgation.
6. Developing operational plans for each proposed RAMP, including:
    a. estimating billets needed,
    b. outlining budget considerations, and
    c. developing plans for interim RAMP functioning, i.e., transition plans for establishing a RAMP prior to the completion of DITTO.
7. Overseeing efforts to maximize coordination of current initiatives such as the Joint Personnel Adjudication System (JPAS), “phasing” (in which information obtained early in a periodic reinvestigation is used to guide the second phase of the investigation), and the Automated Continuing Evaluation System (ACES); and communicating with the Chief Information Officers Council regarding government-wide IT issues that apply.
8. Deciding on the pursuit of related RAMPs/DITTO R&D projects, such as:
    a. developing an Adjudication Decision Support System, and
    b. developing a computer simulation model of the personnel security system.

The recommendation for establishing a managing committee is an acknowledgement that, although a specific vision is necessary for productive discourse and planning, success depends on effective execution. By managing the review and implementation of the tasks outlined above, we believe the APSOC can coordinate the interests of the DoD components, drive visionary and practical improvements throughout the DoD personnel security community, and strengthen the program's ability to serve DoD.

Table of Contents

List of Figures

List of Tables

Introduction

The significant problems we face cannot be solved by the same level of thinking that created them. Albert Einstein

The personnel security program is essential to the mission of the Department of Defense (DoD). The Department employs nearly two and a half million military, DoD civilian, and contractor personnel in positions in which they could compromise national security due to their access to sensitive information. DoD needs personnel who can be entrusted with access to sensitive information and environments. The changes implied in the model presented in this report are designed to improve the overall effectiveness, efficiency, and adaptability of the personnel security program.

Tasking

The Deputy Assistant Secretary of Defense for Security and Information Operations, Command, Control, Communications, and Intelligence (DASD [S&IO/C3I]) initiated a project entitled *Options for Future Defense Personnel Security Systems* (the "Options project") in July 2000. The DASD tasked PERSEREC to consider past initiatives, current problems, and future challenges in a "big picture" study of personnel security. The goal of the Options project was to articulate a model for the personnel security system that would substantially improve the ability of DoD to manage the challenges of the coming decade and beyond. The model should address the main components of the system: requirements for background investigations and periodic reviews, investigative processes, adjudicative processes, and supporting information technologies. It should also reflect best business practices applicable to the personnel security system. In essence, the task was to go beyond a patch-on-patch approach of handling problems in the current mélange of procedures, and to apply a new level of thinking toward designing a better, more coherent system.

Approach

Deficiencies in the DoD personnel security program are well documented. Over the past 15 years, 17 audits or research studies of the program have been done—13 during 1999, 2000, and 2001 alone. These studies describe the problems and offer snapshots of solutions recommended at different points in time for different parts of the system. In October 2000 a DoD Process Review Team (PRT) surveyed these studies and compiled the recommendations from past reports. The PRT then researched the extent of response to the recommendations: what had been done thus far, what was in process, and what had not been done (Personnel Security Investigations Process Review Team, 2000b).

To develop a new model for the organization of the personnel security system, we built on these past studies, making use of the PRT's recent work as well as recent congressional hearings regarding the personnel security system (Defense Security Service, 2001; Defense Security Service, 2000). We used the DoD Draft Strategic Plan (Defense Personnel Security Research Center, 2000) as our guide for the standards a new system should meet. We paid special attention to the best aspects of the current program as well as to programs under development to ensure that the proposed model would capitalize on current strengths and be amenable to promising programs on the horizon, such as the Joint Personnel Adjudication System (JPAS), “phasing” (in which information obtained early in a periodic reinvestigation is used to guide the second phase of the investigation), and the Automated Continuing Evaluation System (ACES). We consulted many experts who shared their expertise with us including staff members and managers at the office of the Deputy Assistant Secretary of Defense (C3I/S&IO), the Office of Personnel Management, the Department of Energy, the U.S. Air Force, the U.S. Navy, the U.S. Army, the Washington Headquarters Service, the Defense Security Service, and the Aerospace Industries Association. After comparing and integrating the information from these experts with relevant published research and government reports, we identified the goals and needs of the various stakeholders and integrated them in a new model. In May and June 2001 we presented the proposed model to policymakers in ASD (C3I), military services, DSS, and others. This report documents research conducted for the Options project, articulates a model for a new personnel security system taking into consideration the current system and other federal personnel security practices, describes organizational roles in the proposed system, offers several suggestions for operational improvements, illustrates how the proposed system would perform in response to an unforeseen surge in personnel security requirements, and outlines recommendations and considerations regarding implementation.

Overview of the Current Personnel Security System

Recent Problems

The current DoD personnel security program dates from the early Cold War with the issuance in 1953 of Executive Order 10450, “Security Requirements for Government Employees” by President Eisenhower. This Executive Order required that all prospective federal employees undergo a specified investigation into their backgrounds: the more risk to national security a federal job held, the more rigorous an investigation would be performed, but the minimum mandated assessments included national and local agency checks (5 U.S.C. 7311, note). The Order spelled out criteria (such as past criminal acts, evidence of mental illness, illegal drug use, or association with groups labeled subversive), to guide decisions about a prospective employee’s qualification for employment. With modifications over the years, many of these criteria still guide adjudication decisions.

The collapse of the Soviet Union in 1991, and with it the end of the Cold War that provoked EO 10450, changed the context of personnel security. Globalization and advances in information technology required new approaches to many personnel security procedures that are now 50 years old. Phenomena such as instant global information exchange, automated data systems using networked databases, and dual use technologies that confound the distinction between military and commercial applications, challenge government’s control of national security information in ways not imagined in 1953. As globalization rapidly reframes economic relationships between nations, the world politics of the bipolar Cold War era has become more complex. For example, national allegiance has taken on new meaning with the relatively easy immigration of professionals to the United States and the on-going ties they maintain to their countries of origin (Personnel Security Managers’ Research Program, 2002). The personnel security program has struggled to respond to these changing conditions.

The program has been hampered in this response during the last decade by shrinking resources and unfortunate management decisions, such as a poor strategy for shifting to a different automated information processing system. In the early 1990s, cuts to DoD budgets touched off several rounds of personnel cuts at the Department's designated investigation agency, the Defense Investigation Service (DIS). In 1992 DIS enlarged its mission to include counterintelligence and in 1997 changed its name to the Defense Security Service (DSS), but its responsibilities outpaced the resources it received. Policy changes in the mid-1990s, including an increase in the investigative requirements for military accessions and a reduction in the time interval between periodic reinvestigations (PRs) for Secret clearances, added to the demands placed on DSS. The agency's shift in 1997 to an unstable automated information system touched off lingering problems and led to lengthy completion times for background investigations and a snowballing backlog of PRs that could not be completed within the time limits. By late 1999, the backlog in investigations had reached urgent proportions: requests for Top Secret PRs were postponed past the 5-year mark required by law, and military commanders and civilian agencies in DoD could not staff their organizations with the cleared personnel they needed. Although DSS has worked hard to recover from these setbacks, its problems exacerbated other weaknesses in the DoD personnel security system that had become overloaded, technologically outdated, and under-funded. (Personnel Security Investigations Process Review Team, 2000a; Personnel Security Investigations Process Review Team, 2000b; Bosshardt, 2000; Threats to National Security, 1998).

Symptoms of this simmering crisis in the current personnel security system included the backlog of thousands of new and periodic background investigations, delays in granting clearances that ran from months into years, lagging data collection and information management technologies that did not meet current standards for information systems, and a lack of standardization, prioritization, and flexibility across the system. This is the confluence of problems that the Options project was asked to address in a vision of a better system. Despite numerous studies of the problems done since 1985, and many well-founded recommendations in these studies, attempts at solutions have too often been reactive, piecemeal, and only partially implemented. As summed up by the ranking member of the Subcommittee on National Security, Veterans' Affairs and International Relations, "it seems to me that we have a system that is designed to fail." (Defense Security Service, 2001a).

Although the DoD personnel security program has been inundated by problems, it has also been buoyed by the progress made recently in a series of new initiatives including the Joint Personnel Assessment System (JPAS) and the Automated Continuing Evaluation System (ACES). What follows is a brief overview of the existing procedures in the current DoD personnel security system. We also compare DoD's program with several other federal personnel security programs to survey the variety of possible approaches already in place across the federal government. We then discuss attributes that are necessary in an ideal personnel program and describe the model program we propose for the future. Proposals for an improved model will be based on this foundation of understanding the attributes of ideal and current systems.

The Current DoD Personnel Security Program

The federal government has used security clearances to control access to national security information for decades. DoD is the largest of 13 federal agencies that grant security clearances. In outline, the processing of an initial DoD security clearance consists of a request from an official, a personal information questionnaire, a background investigation, a written report on the results of the investigation, an adjudication decision based on the report, and a series of due process procedures. Table 1 lists the levels of security clearances currently granted in DoD and the scope of background investigations specified for each level.

After a clearance is granted, the individuals with Top Secret, Secret, or Confidential clearances are subject to periodic reinvestigation, during which another background investigation is done to monitor changes and to re-certify the person's fitness to hold a clearance. As Table 1 shows, for a Top Secret clearance this reinvestigation is to be done within five years, Secret clearances require 10-year reinvestigations, and Confidential clearances require 15-year reinvestigations. Two levels of security—military accessions based solely on an ENTNAC and "Trust" level security access—do not require periodic reinvestigations.

When the backlog crisis hit in 1999, some of DoD's background investigations were shifted from DSS to the Office of Personnel Management (OPM). Meant as a temporary expedient until the crisis was resolved, from 1999 to 2002 an increasing proportion of DoD background investigations were done by OPM. In 2002 OPM, through its sole contractor for investigations, the United Security Investigations Service (USIS), is projected to investigate at least half of DoD's personnel security cases (C3I Integrated Process Team, 2002). DSS also began to employ private companies of contract investigators in addition to OPM. A description of DoD's current system therefore must take into account the fact that the typical procedures, in which DSS provided background investigations for DoD, are now complicated by several atypical expedients adopted recently to meet the backlog, including the shifting of many investigations to OPM and the contracting for investigations with other private firms.

The current DoD personnel security program (see Figure 1) begins in the field, in the offices of military commands, civilian agencies, or contractors, with a need for trustworthy employees, many of whom work with classified information. Thousands of separate decisions (requests) by officials in the field together make up the "requirements" for background investigations and clearances. Thus, requests for clearances are decentralized, and the magnitude of requests is open-ended. Little effort is made to limit or ration them, or even to require justification for them. The current system assumes that all requests will be met within the legal time frames, yet the cutbacks in resources provided to accomplish this over the past decade suggest that this assumption may be unwarranted.

To outline procedures in background investigations, we will describe those at DSS, DoD's designated investigation agency. Differences between approaches taken by DSS and by OPM are detailed in Appendix A where the two investigation providers are compared.

Table 1
DoD Personnel Security Clearances: Scope

Level of Access	Initial Investigation	Periodic Reinvestigation
Top Secret–Sensitive Compartmented Information (TS-SCI)	Single Scope Background Investigation (SSBI)	Top Secret Periodic Reinvestigation (TS-PR) Within 5 years
Top Secret–Special Access Program (TS-SAP)	Single Scope Background Investigation (SSBI)	Top Secret Periodic Reinvestigation (TS-PR) Within 5 years
Top Secret (TS)	Single Scope Background Investigation (SSBI)	Top Secret Periodic Reinvestigation (TS-PR) Within 5 years
Secret (S)	National Agency Check with Local Agency Checks and Credit Check (NACLC)	Secret Periodic Reinvestigation (S-PR) Within 10 years
Confidential (C)	National Agency Check with Local Agency Checks and Credit Check (NACLC)	Confidential Periodic Reinvestigation (C-PR) Within 15 years
Trust	National Agency Check (NAC)	Not required
Military Accession	Entrance National Agency Check (ENTNAC)	Not required

The potential clearance holder, the subject, fills out an SF-86 form, the electronic version of which is the Electronic Personnel Security Questionnaire (EPSQ). It asks for information regarding the person's career, past residences, education, foreign travel, connections, and other personal matters that provide starting points for the background investigation. The form typically would go to the DSS Personnel Investigations Center (PIC) in Fort Meade, MD where an intake specialist checks it for completeness and returns to the requestor forms that are missing information. Once a complete form is submitted, one of approximately 150 DSS case analysts "scopes" the investigation by assigning parts of the investigation to one or more of the roughly 80 DSS field offices, depending on where the subject has lived, worked, and gone to school. The case analyst sends out "agent lead sheets" to DSS field offices that outline the facts to be checked, and a field investigator gathers information about the leads. If the subject has lived in several places, several field offices from those various locations may check the leads.

There are provisions, outlined in the DoD Regulation 5200.2-R, for granting interim collateral security clearances before all the required investigative procedures have been completed. For military and civilian DoD employees, when a requestor needs an interim clearance for a subject, he or she typically asks adjudicators at the relevant CAF to monitor the progress of an investigation and to adjudicate an interim clearance once the following elements are in place: the subject's EPSQ has been reviewed, results of the checks for criminal history at national and local agencies have been returned and reviewed, the single-scope background investigation has been initiated, and local base police and personnel records have been checked. In rare cases where delay could impair national security, the head of a unit in the field requesting the access may, after reviewing the same information, grant an interim clearance. For SCI access, only an adjudicator at an appropriate CAF may grant an interim clearance. In the case of access by industrial contractors, the Defense Industrial Security Clearance Center (DISCO) grants or denies interim clearances to clean cases based on the EPSQ and agency checks, and informs the industrial requestor of the adjudication.

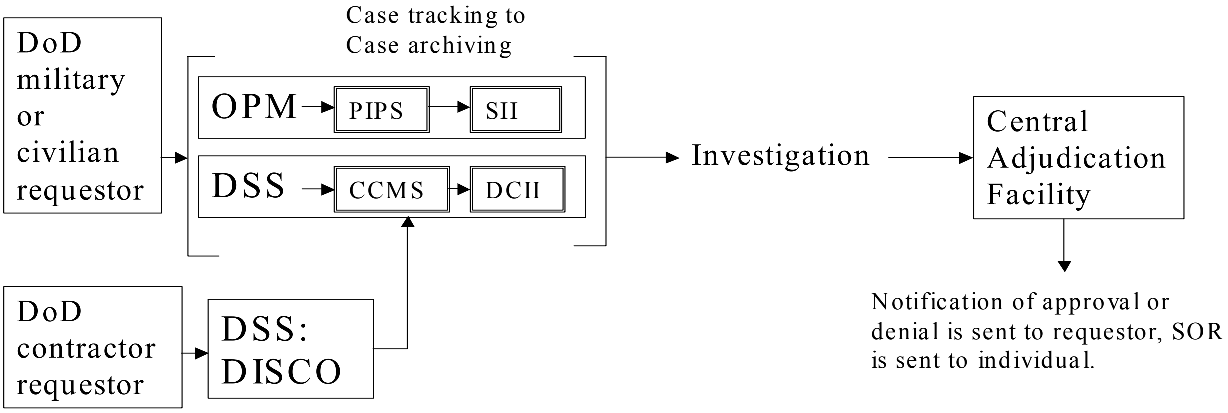

DoD military or civilian requestor
Case tracking to
Case archiving
OPM
PIPS
SII
DSS
CCMS
DCII
Investigation
Central Adjudication Facility
Notification of approval or denial is sent to requestor, SOR is sent to individual.
DoD contractor requestor
DSS: DISCO

Figure 1 Overview of the Current DoD Personnel Security Process.

If an issue arises during an investigation that calls into question the trustworthiness of the subject, the investigator must expand the inquiry to supply enough information for an adjudicator to resolve the issue and make a decision on the clearance. As leads are completed, the information is sent to the case analyst at the PIC, who decides when investigative criteria have been met and when sufficient information has been provided to resolve potential issues. Meanwhile, the PIC case analyst requests information on the individual from national agencies, including law enforcement agencies and courts in areas where the person has lived, the Federal Bureau of Investigation, the Central Intelligence Agency, the Bureau of Immigration and Naturalization, and OPM. The analyst also checks the subject's financial records through credit bureaus, banks, and other financial databases. Having amassed this information, the case analyst compiles it into a report and forwards it to the appropriate adjudication facility for a decision.

Before 1993, authority to make adjudication decisions was widely dispersed across DoD among the various components and agencies. A trend toward consolidation that began in 1965 with the location of all industrial adjudication decisions at the Defense Industrial Security Clearance Review (DISCR) office, slowly moved DoD away from the view that security clearances should be handled at a component level. Although the military services and DoD agencies gradually gave up some control over investigations and adjudications for their own people, as of 1989 there were still 19 offices making adjudications. During this period, commissions periodically urged reform in the direction of more consolidation in order to increase efficiency. An early reform effort in 1972 resulted in the merging of investigative agencies and creation of the Defense Investigation Service (DIS) to handle all DoD background investigations. During the 1980s, as espionage by American citizens captured headlines and focused attention on the personnel security system, more reforms were proposed. For example, the DoD regulation 5200.2-R in 1987 stated that "to ensure uniform application of the requirement of this Regulation and to ensure that DOD personnel security determinations are effected consistent with existing statutes and Executive orders, the head of each Military Department and Defense Agencies shall establish a single Central Adjudication Facility for his/her component" (Department of Defense, 1987). Although some consolidation was achieved, studies cited a demonstrable lack of consistency among the resulting 19 agencies that led to unfairness and a lack of due process for the individual. In 1993 a major reform aimed at increasing efficiency and consistency further consolidated the various adjudication agencies into eight "Centralized Adjudication Facilities" (CAFs) along agency lines.[2]

Adjudicators at the CAFs consider information provided in the investigative "report of investigation," weighing the background information and records checks collected during the investigation against the 13 National Adjudicative Guidelines (Exec. Order No. 12968, 1997).[3] These guidelines are also the result of a reform aimed at improving consistency, but here the consistency is not only in decisions made across DoD components, but also across federal agencies in order to achieve reciprocity between the clearances granted by the various DoD and non-DoD agencies. DoD adjudicators began to use the new guidelines in review form in 1996. In March of 1997 the guidelines were promulgated by executive order, and DoD formally adopted them in November 1998. The guidelines direct adjudicators to consider the "whole person," that is, favorable as well as unfavorable and past as well as present information, to make a judgment about the potential trustworthiness of an individual. There are roughly 200 adjudicators spread among the eight CAFs. DoD adjudicators make clearance determinations on all clearances. They make roughly 400,000 decisions per year.

If adjudication is favorable, notice is sent back to the requesting office and the individual receives notice of the clearance from the local security manager there. If the decision is unfavorable, due process procedures are available. These vary slightly depending on whether the individual is military, government civilian, or a contractor employee. In general, to appeal unfavorable clearance adjudication, a person can either respond in writing to the appropriate Personnel Security Appeal Board[4] (PSAB), or can request a personal appearance before an administrative judge (AJ) at the Defense Office of Hearings and Appeals (DOHA). If the person opts for a hearing, the AJ conducts it and sends a recommendation to the person's PSAB, which then makes a decision on the appeal based on the hearing and evidence collected on the individual. A second layer of appeal is offered to contractor employees, who can appeal an AJ's unfavorable recommendation to a DOHA Appeal Board, which makes the final determination.

As OPM performed an increasing proportion of DoD background investigations, an element of complexity was added due to multiple federal agencies working on DoD background

[2] The current 8 Centralized Adjudication Facilities are: the Air Force Central Adjudication Facility, the Army Central Personnel Security Clearance Facility, the Defense Intelligence Agency Central Adjudication Facility, the Directorate of Management, Joint Chiefs of Staff Central Adjudication Facility, the Department of the Navy Central Adjudication Facility, The National Security Agency Central Adjudication Facility, the Washington Headquarters Services Consolidated Adjudication Facility, and for industrial clearances, the Defense Industrial Security Clearance Office, now a part of the Defense Security Service, in conjunction with the Defense Office of Hearings and Appeals, which is in the Defense Legal Services Agency.

[3] E.O. 12968, Sec. 3.2(b) August 2, 1995; Security Policy Board, "Uniform Adjudicative Guidelines," March 24, 1997. 32 C.F.R. Part 47, Subpart B.

[4] There are six Personnel Security Appeal Boards for: Army, Navy, Air Force, Defense Intelligence Agency, National Security Agency, and Washington Headquarters Service. WHS handles appeals for all DoD civilian agencies other than DIA and NSA.

investigations,[5] e.g., implementing policy guidance consistently across DoD and non-DoD investigative agencies, and multiple agencies with different information systems updating and consulting the Defense Clearance and Investigations Index (DCII). In addition to DoD's specific need for supplementary investigative support to assist DSS, there has been a general trend in the federal government to contract with private companies for services rather than to hire federal employees. This is a second factor leading to multiple providers of investigations. The drive to outsource nongovernmental functions has been strong since the early 1990s. As the backlog crisis at DSS developed late in that decade, examples of many other federal agencies shifting specific work to private contractors were salient. DSS contracted for background investigations from various private companies, including OMNIPLEX, ManTech, MSM, DynCorp, and GBSG, and some of these companies continue to do background investigations for DSS in FY2002.

Thus an anomalous situation developed for DSS caused by cutbacks, management decisions, and premature deployment of its automated case tracking system. To respond to its backlog of investigations, DSS became a monitor of contractor investigations, but this shift has generated issues of consistency and quality of background investigations among the various providers. It has also generated incompatibilities in automated case tracking and management reporting, since the various agencies and companies use different computer systems. In addition, in order to respond to the felt need for more institutional structure to support tracking of industry clearance requests from the many DoD contractors that submit them, DSS has implemented a Central Requirements Office. Among the main questions the Options project has considered are what roles DSS is best suited to play in providing personnel security investigations for DoD, what temporary expedients and tasks that it has taken on in the current crisis it should give up, and which agencies should take on the necessary functions. To gather data on this series of interrelated questions, we compared the current personnel security practices of several DoD and intelligence agencies. A summary of the comparison is given here.

Comparison of Investigation and Adjudication Across Federal Agencies

We compared the practices of five representative federal agencies that do background investigations or adjudications of security clearances: DoD's DSS, OPM, the Department of Energy (DOE), the Central Intelligence Agency (CIA), and the National Reconnaissance Office (NRO).

Overall, we found several important differences in procedures and assumptions across federal personnel security programs, implying that there is a range of workable approaches to procuring a trustworthy workforce. Among the dimensions along which these procedures vary are: the co-location or physical separation of functional specialties within the system, and the consequent ease of interaction between specialists; the scale of the task, (i.e., the volume of clearances that must be processed by a given agency and how long processing takes); the degree to which processing of clearances relies on information technology; the degree of reliance on in-house investigators as opposed to contractor investigators; whether "clean case screening"

[5] Because DSS has opened all cases that were previously backlogged, current (2002) planning calls for OPM to gradually shift specified categories of investigations back to DSS through FY03. (C3I Integrated Process Team, 2002).

procedures are used; and certain distinctive features of these agencies that affect their procedures (see Appendix A for details of the comparison).

Among these dimensions, the volume of clearances dictates general parameters for what is operationally feasible in a personnel security system. In 2000, some 2.1 million DoD personnel held security clearances, whereas DOE accounted for approximately 105,000 clearances; NRO and CIA are both smaller, though the size of their workforces remains classified. A relatively small agency focused on specific missions can approach the vetting and monitoring of its employees differently than can a large organization like DoD. DoD's need to track millions of cases, archive those data, and regularly communicate with far-flung local security managers makes its task different from an agency located largely in one building.

Nevertheless, DoD can learn from and adapt the relevant innovations of others. OPM is an even larger and more varied organization than DoD. OPM is responsible for vetting personnel for many agencies of the federal government. OPM achieves a relatively fast turnaround on background investigations done by USIS by relying on automated scoping routines performed by computer, automated data requests to national agencies, scanable forms filled out by sources in the field to allow rapid capture of data into electronic form, field investigators equipped with laptop computers, and an information system capable of reliably generating various management reports and billing for an investigation as soon as it is scheduled (U.S. Office of Personnel Management Investigations Service, 1999). DSS is working to implement these kinds of automated processes as well. The ideal end-state in an improved personnel security system would feature an information technology office that was fully integrated into all parts of the system to support personnel security processes from "tooth to tail," from data collection in the field and integration of data from various sources, through investigative report, adjudication, notification of outcome, case tracking and archiving of data, to management reports and system oversight. The proposed personnel security system that we describe below includes such an office to integrate automated processes.

Secondly, DoD's practice of strictly separating investigators from adjudicators is not the only model used by these various federal agencies, and other models could be considered. Those who perform background investigations gain valuable insights into a subject that may be only partially captured in a written report. An adjudicator may have questions or concerns that could be most efficiently addressed in direct communication with the investigator. The advantages of closer interaction could be explored through the experiences with it at the CIA, for example. In addition, clean case screening by case analysts—e.g., for interim clearances at DISCO and as part of the 2002 pilot study of phased PRs at DSS[6]—suggests that investigative staff can be relied upon to make limited adjudicative determinations.

The issues that DoD needs to sort out regarding potential interaction between investigators and adjudicators cluster around: [1] what the decisions by adjudicators represent, [2] what are the legal issues, and [3] how to limit the potential for interactions to add significant burdens for the investigative or adjudicative staff. Currently there is broad agreement in DoD that adjudication and investigation should be kept separate. So how should adjudicators be

[6] PR phasing is described below in a subsection below entitled "Integrating Relevant Initiatives."

considered: are they like the members of a jury in a courtroom, weighing evidence and reaching decisions based on it, or are they more like clinical service providers who collect information about a client and make judgments about each client to decide on a course of action? Should adjudicators continue to be kept apart from the investigator, who in the courtroom model is like a police detective who gathers evidence about a defendant, or should investigators and adjudicators be encouraged to consult with each other as a clinician would consult a psychologist, teacher, parents, and whoever else had insights about their client?

Thirdly, DoD can learn from the mere fact that there are such a variety of personnel security procedures at different agencies. Things can be done successfully in more than one way, and more importantly, different agencies need somewhat different procedures to best accomplish their personnel security. Calibrating a balance is necessary between further consolidation, with its promise of efficiency, standardization, and parsimony, and continued component control, with its assurance of responsiveness, closer fit with unique needs, and control over resources. The Options project model we propose re-calibrates and improves this balance.

A Future Defense Personnel Security System

Our thinking about the future personnel security system for DoD has been guided by principles of organizational effectiveness and fundamental goals we believe the system should strive to attain. These goals relate to proposals for new organizational designs and business roles, as well as to the need for integrating and improving superior parts of the current system. Collectively, as described below, they comprise ideal attributes for a future DoD personnel security system.

Ideal Attributes of a DoD Personnel Security System

The attributes described in this section represent an initial set of assumptions that are necessary but not sufficient for guiding the development of an improved personnel security system. Ideal attributes must be considered in the context of an overall model and vision of specific organizational roles, supporting IT, and workflow scenarios to productively guide development of a more coherent personnel security system. Thus, we discuss ideal attributes of a personnel security system followed by a description of an organizational model that would reify them.

New Organizational Designs and Roles

Each DoD component should exert control over and have responsibility for determining the funding, prioritizing, and management of its own personnel security requirements. The Secretary of each military service is charged with the ultimate authority for granting security clearance for personnel in that component. Coordinating major responsibilities within the components would localize and strengthen responsibility where damage from failures of personnel security would strike and where requests for clearances are generated and adjudicated.

Complementing this shift of initiative to components, we argue that a DoD office should be created to operate, budget for, and evaluate an information technology (IT) architecture to serve the personnel security system. An integrated IT system should tie the components together and support rapid and secure data exchange and retrieval, functional evaluation, and data-based modeling and prediction.

Thirdly, a new structure for systemic oversight should be framed in the form of a policy-making committee made up of flag-level representatives from the components, and chaired by a C3I S&IO SES-level Director. This group should be charged with responsibility for overseeing the DoD personnel security system.

The DoD personnel security system should also continue to invest in infrastructure that will allow it to capitalize on data mining techniques, both for background investigations and for continuous monitoring of cleared personnel. The advances being made in linking databases provide opportunities to extend personnel security investigation and monitoring techniques.

Furthermore, major parts of the DoD personnel security system should be designed to be scalable over time and flexible enough to accommodate sudden demands. New elements of the system should be framed with inevitable change in mind, so that the size or number of elements can be cut back or increased as circumstances warrant. Flexibility to rapidly increase capacity to clear personnel in the event of a military emergency should likewise be built into the system.

Integrating and Improving Good Parts of the System

Several of our goals for DoD's personnel security system are consistent with a core theme underlying the development of an improved model: maintaining, integrating, and extending valued parts of the current system. Adjudication of security clearances should express DoD policies while it supports the mission of each component. Agencies should continue to move to automation and machine-readable formats that can reduce manual handling and facilitate workflow of data. The conduct of background investigations should be kept organizationally distinct from the adjudication that makes use of information gathered by investigations, but enabling interaction between investigators and adjudicators may prove fruitful.

Three important initiatives, JPAS, Phased PR Investigations, and ACES, are currently under development or in an early stage of implementation in the DoD. These initiatives hold the potential to significantly improve the personnel security process and provide essential blocks on which to build the structure of the proposed model.

Joint Personnel Adjudication System (JPAS). JPAS represents the virtual consolidation of the DoD CAFs. When fully implemented,[7] JPAS will use a centralized database with centralized computer processing and application programs for standardized DoD personnel security processes that relate to adjudication, such as: [1] automating both core and CAF-unique functionality, [2] providing "real-time" information regarding clearance, access, and investigative status to security personnel and authorized organizations, e.g., DSS, Defense Manpower Data Center, Defense Civilian Personnel Management System, OPM, and Air Force

[7] As of Spring 2002, JPAS status is Initial Operating Capability. A Final Operating Capability date has not been determined.

Personnel Center, and [3] providing comprehensive and up-to-date reporting capabilities across adjudicative activities (JPAS, 2001). JPAS will be a core capability of the system-wide IT architecture that supports the goal of linking and sharing important electronic databases proposed in the model. Planning for integration of JPAS and other essential systems into that larger architecture will be the essential.

Phased Periodic Reinvestigation (Phasing). Based on the most comprehensive study of the SSBI-PR conducted to date, PERSEREC proposed a new approach that would expedite the periodic reinvestigation, cut costs, e.g., PBD434 estimates savings of $34M in FY03, and improve security by enabling a more productive allocation of investigative resources. Because research on SSBI-PRs has shown that potential issue cases can be distinguished from clean cases early in the periodic reinvestigation, it is possible to take a risk-management approach to scoping the reinvestigation. Fewer resources can be devoted to low-risk clean cases, with the saved resources reallocated to other, more productive measures (such as ACES, below) designed to reduce personnel security risk (Heuer and Crawford, 2001). These improvements can be achieved through a "phased reinvestigation" in which information obtained early in the investigation (phase 1) is used to guide the scope of subsequent investigation (phase 2). Pilot tests indicate that case analysts can effectively evaluate when phase 1 investigative results necessitate expansion to phase 2. The proposed model could readily accommodate this promising approach, and would likely add to its cost-effectiveness through plans for greater IT use and integration.

Automated Continuing Evaluation System (ACES). PERSEREC's ACES project will provide a system for automated checks of key government and commercial databases, e.g., personnel security questionnaire records, national credit vendor databases, FBI criminal history files, U.S. Customs databases on foreign travel, and federal court records, in order to identify cleared personnel who may be engaging in acts of security concern in between regular personnel security investigations (Chandler and Timm, 2001). When fully implemented[8] ACES will greatly enhance access to and assessment of security relevant information sources on cleared personnel for use by JPAS and other authorized agencies. As with JPAS, the data mining capability provided by ACES is consistent with several ideal attributes underlying the proposed model of business processes and information flow. The system-wide IT architecture in the proposed model will facilitate the operation of ACES.

Aspects Needed in Any Effective Personnel Security System

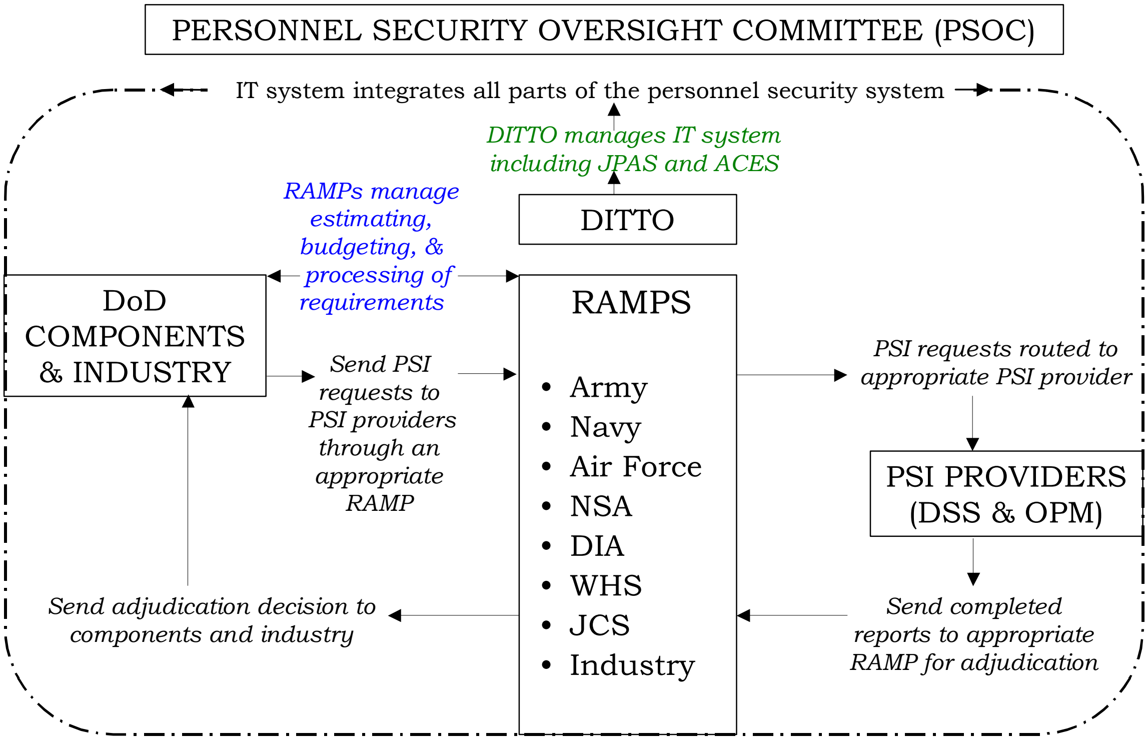
Accountability for performance should be clearly defined throughout the system. Personnel security policies should be appropriately researched with respect to their intended effect and congruity with related policy, and supported with adequate resources. Payment from components should be linked to services provided. In addition, an effective system should strive to: [1] manage and minimize risk to national security, [2] maintain quality, speed, consistency, fairness, cost-effectiveness, and predictability across its elements, and [3] be amenable to standardized measurement, ongoing evaluation, and improvements as needed. Finally,

[8] As of Spring 2002, Interface Control Documents regarding communications and data transfers between JPAS and ACES were under development. ACES alpha and beta testing are scheduled to be completed by March 2003. Initial Operating Capability is scheduled for June 2003.

reciprocity across DoD components and agencies should be maximized, recognizing that this goal is not as simple as it sounds among organizations with aspects in common but also with aspects that are distinctive.

Organizational Elements of the "RAMPs/DITTO" Model

The proposed personnel security system model (Figure 2) includes five organizational elements, each of which is described in a subsequent section of this report. Three of the five elements, Requirements and Adjudication Management Programs (RAMPs), the Defense Investigation Technology and Tracking Office (DITTO), and the Personnel Security Oversight Committee (PSOC) are proposed new organizational entities.


PERSONNEL SECURITY OVERSIGHT COMMITTEE (PSOC)
IT system integrates all parts of the personnel security system
DITTO manages IT system including JPAS and ACES
DITTO
RAMPs manage estimating, budgeting, & processing of requirements
DoD COMPONENTS & INDUSTRY
Send PSI requests to PSI providers through an appropriate RAMP
RAMPS
• Army
• Navy
• Air Force
• NSA
• DIA
• WHS
• JCS
• Industry
PSI requests routed to appropriate PSI provider
PSI PROVIDERS (DSS & OPM)
Send completed reports to appropriate RAMP for adjudication
Send adjudication decision to components and industry

RAMP: Requirements & Adjudication Management Program
DITTO: Defense Investigation Technology & Tracking Office

Figure 2 Proposed DoD Personnel Security System: The RAMPs/DITTO Model.

Figure 2 illustrates the basic relationships among organizational elements of the RAMPs/DITTO model. The following sections of this report provide details for each element and its functions, as well as improved business processes enabled by the RAMPs/DITTO model.

DoD Components and Industry

The RAMPs/DITTO model includes an element entitled "DoD Components and Industry" to represent the full set of organizations that currently request investigations and adjudications from the DoD personnel security program. "Industry" refers to organizations with employees who are required to have personnel security investigations to be eligible to perform contract work for DoD. "DoD Components" refers to the Office of the Secretary of Defense, all military departments, Joint Chiefs of Staff, Combatant Commands, Inspector General of DoD, Defense Agencies, DoD Field Activities, and all other organizational entities within the Department of Defense. For the purposes of this report, we also include several non-DoD government entities, such as the GAO and the Library of Congress, that currently use the DoD personnel security program. The list of government entities that request personnel security investigations from DoD includes:

- Army
- Navy
- Air Force
- Marines
- Coast Guard
- DIA: Defense Intelligence Agency
- NSA: National Security Agency
- JCS: Joint Chiefs of Staff
- WHS: Washington Headquarters Services
- White House (for DoD assignees only)
- DARPA: Defense Advanced Research Projects Agency
- DISA: Defense Information Systems Agency
- DISCO: Defense Industrial Security Clearance Office
- DOHA: Defense Office of Hearing and Appeal
- DLA: Defense Logistics Agency
- DeCA: Defense Commissary Agency
- DSCA: Defense Security Cooperation Agency
- DFAS: Defense Finance & Accounting Services
- DCAA: Defense Contract Audit Agency
- DTRA: Defense Threat Reduction Agency
- LOC: Library of Congress
- NIMA: National Imagery and Mapping Agency
- OSD: Office of the Secretary of Defense
- USMEPCOM: Military Entrance Processing Command
- DODIG: Department of Defense Inspector General
- GAO: General Accounting Office
- DSS: Defense Security Service

Based on the DSS (2000/2001) "Data Call", approximately 76 percent of all PSI requests come from the military services, 12 percent from industry, and 2 percent from NSA and DISA. The remaining 10 percent of requests come from all other government entities combined. Because industry and the DoD components constitute the organizational entities that rely on PSI related services from the DoD personnel security program, the RAMPs/DITTO model includes these organizational entities.

Requirements and Adjudication Management Programs (RAMPs)

Organizational systems operate best to the extent that there is coordination among the following dimensions: management, authority, resources, and accountability. In the current DoD personnel security program, these dimensions are divided among DSS, the DoD components and industry, and OSD/C3I in ways that repeatedly hinder effective operations. For example, although DSS is often held accountable for assessing and predicting total DoD personnel security requirements, the responsibility for planning and programming such requirements rests with the DoD components and industry. And although the components and industry are essentially the "customers" who request investigative services, they neither determine nor manage the resources necessary to ensure the delivery of satisfactory investigations. In 2001 congressional testimony addressing these issues the DASD [C3I/SI&O] overseeing the personnel security program indicated that "there is no centralized focal point for the services on the front end" (Defense Security Service, 2001c).

Because the military services currently are the largest customers for PSI services and because the service secretaries have legal authority over final access determinations, it would be both logical and practical to coordinate much of the management, authority, resources, and accountability for personnel security through service-level organizations, and to use a parallel model for other DoD components and industry. The organizational entity we propose for this coordination is the *Requirements and Adjudication Management Program*.

As shown in Figure 2, we propose the creation of eight RAMPs to parallel the arrangement of Central Adjudication Facilities (CAFs) that currently serve DoD components and industry. Each RAMP would be responsible for the following six functions:

1. Managing estimation of PSI requirements, including out years, through interactions with commands and/or organizational liaisons.
2. Managing the requirements budget and ongoing rate of utilization for the organization(s) it serves.
3. Setting processing priorities for personnel requirements within the organization(s) it serves.
4. Adjudicating clearances by means of an internal adjudication facility.
5. Assigning adjudicators to PSI cases during investigation—the *Case Team* approach.
6. Acting as the single point of contact and help desk for the organization(s) it serves.

We now describe each of these six functions.

Managing Estimation of PSI Requirements, Including Out Years, Through Interactions with Commands and/or Organizational Liaisons

The military services need to plan for their personnel security requirements—for at least two out-years—based on as many as possible of the following factors: [1] anticipated force structure, [2] an understanding of which occupational positions should include access to classified or sensitive material, [3] projections of demographic trends (e.g., relevant turnover and retirement rates), and [4] other plans that relate to personnel security needs (e.g., anticipated projects that may require substantial increases in cleared personnel).

The three most important justifications for proposing eight RAMPs—Army, Navy, Air Force, National Security Agency (NSA), Defense Intelligence Agency (DIA), Washington Headquarters Service (WHS), Joint Chiefs of Staff (JCS), and industry—each staffed with component-specific experts are: [1] accurate projections of requirements is critical to the planning, programming, and budgeting processes of each of the largest DoD components, [2] the input data and mathematical model for projections is unique for each military service, major component agency, and industry and [3] the task of developing, updating, and analyzing an accurate projection model for a particular component is best performed by staff who are well-informed of the needs, operations, organizational liaisons, and informational resources of that component.

Each RAMP director would be at a level commensurate with the responsibilities of overseeing the management, estimation, and processing of personnel security requirements for one of the eight organizations described above, for overseeing relevant adjudications, and for interacting with the senior DoD leadership charged with overall management and policy.

The "industry RAMP" would combine the functions of DSS's Central Requirements Office (CRO) and some of the functions of the Defense Office of Hearings and Appeals (DOHA). The industry RAMP could report to the DSS Directorate for Industrial Security Programs, which currently oversees several activities of the National Industrial Security Program (NISP), or to some other appropriate agency. Because industry requirements presents unique and important challenges—such as assessing requirements from over 11,000 DoD contracting facilities at which cleared personnel often work on projects for more than one DoD component—addressing these challenges by staffing a dedicated (RAMP) office with industry experts and a Director responsible for supervising and coordinating all industry-related operations is likely to facilitate effective understanding and execution of personnel security for DoD.

No reliable method is currently in place to predict DoD personnel security requirements. Without this ability, it is difficult for DoD to budget accurately for investigative and adjudicative work, or forecast the effects of policy changes on the personnel security program. Although conducting the research necessary to develop a complete PSI requirements prediction model was beyond the scope of the Options project, we collected important information about current practices by commissioning a small-scale *Survey of Methods and Plans for Projecting Personnel Security Investigations Requirements* (Marshall-Mies, 2001).

Current Methods for Determining Personnel Security Requirements. The goals of the *Survey of Methods and Plans* study were to document: [1] methods that DoD organizations (military services, defense agencies, and defense contractors) currently use to project PSI requirements, and [2] efforts being undertaken by several DoD organizations to improve current and historical personnel security databases and develop organization-specific PSI requirements projection models. Ten DoD contractors, three military services, and two government agencies were selected to participate in this effort because their projected PSI requirements were among the highest within the DoD for the years 2002 through 2007. Projections for these organizations included initial investigations and PRs for positions requiring access to Sensitive Compartmented, Top Secret, Secret, and Confidential Information and for positions designated as Positions of Trust. Military service projections included requirements for Entrance National Agency Checks (ENTNACs) for military accessions and NAC(T)s for Positions of Trust. Respondents who participated in telephone interviews were individuals responsible in 2001 for providing DSS with their organizations' projected PSI requirements for the years 2002 through 2007. They were asked to provide insights and suggestions concerning how their organization generated these estimates and what data and methods might be available to improve future estimates. An overview of study findings is presented below, and additional details of the study's methodology and results appear in Appendix B. The complete report is available from PERSEREC.

The findings from this study suggest that several steps are needed to improve the accuracy of DoD personnel security requirements projections. First, most organizations, especially the military services and government agencies, need to improve their current databases of cleared personnel. These databases need to contain accurate and up-to-date records of all currently cleared personnel, their date(s) of investigation, and the level of access required in their present position. In addition, these databases need to incorporate or be linked to other personnel data, such as assignment transfers, so they can reflect personnel actions on a real-time basis. As part of this effort, existing software may need to be modified or new software developed so that individuals in appropriate need-to-know positions, such as investigators, adjudicators, security officers, and OSD research and administrative staff, can easily query these databases. JPAS promises to be a major contributor in this area. These kinds of database development efforts will improve baseline data that could serve as a starting point for projecting PSI requirements.

DoD organizations and contractors will also need to identify and understand the interactions of key variables that affect current and future PSI requirements. Such variables include historical and anticipated accessions (for military services), attrition and retirement rates, anticipated growth or downsizing, movement of personnel between positions requiring and not requiring access, and new business or changing requirements. Once organizations have accurate and current data on cleared personnel and understand how key variables impact their present and future PSI requirements, they will be in a better position to develop organization-specific models for projecting PSI requirements.

Three initiatives—by the Army, Air Force, and Defense Security Service's Central Requirements Office—are currently underway to improve the assessment and projection of PSI requirements. The Army is developing an automated *Total Army Personnel Security Investigations Management System* (TAPSIMS). TAPSIMS will count and categorize incoming personnel security requests so that individual Army commanders will have a record of all requests submitted for enlisted personnel and officers in their command (Paller, 2002). This also will improve the quality of data aggregated across subcommands and, in turn, improve the data aggregated from the field for the total Army by Headquarters (Department of the Army, DCS for Intelligence), which is responsible for developing the Army's PSI projections.

An Air Force Headquarters initiative is employing a "Systems Thinking" approach to model the flow of personnel through the Air Force system in an attempt to predict and control the number of background security investigations for the budget year plus two. The objective of this effort is to gain insight on how service policies, attrition, and assignment turnover interact to generate requirements for security investigations. Initially, subject matter experts were used to map the policies and activities that generate the need for background investigations, resulting in an initial model covering the active Air Force (military officer, enlisted, and civilian). Initial tests indicate that this model can provide officials with estimates of the number of investigations required as systems variables change (Marchiori, 2002). In the second phase of development, the active Air Force model will be modified to incorporate unique requirements of the Air Force Reserve and Air National Guard.

The Defense Security Service's Central Requirements Office has initiated surveys of the personnel security requirements of industry. A pilot study, completed in the spring of 2001, solicited estimates for personnel security requirements and comments on how the estimates were derived—for the years 2002-2007—from approximately 240 of the largest defense contractors. A follow-up study, fielded in the fall of 2001, solicited similar estimates from all (over 11,000) defense contractors (Projection of Personnel Security Requirements for Industry, 2002).

By better describing current requests for investigations, the Army's model should provide solid baseline data for future projections. The Air Force's model should increase our understanding of the interactions among system variables and their impact on PSI requirements. Both efforts may provide critical knowledge and preliminary models for other organizations and for the DoD as it attempts to improve PSI requirements methods and procedures. All three studies (Army, Air Force, and DSS/Industry) should be completed in 2002.

Because findings from the *Survey of Methods and Plans* study highlight the need for DoD organizations, such as the military services, to better develop and link their personnel security databases, these findings are consistent with the proposed model of a personnel security system that includes individual RAMPs supported by an integrated IT network.

Managing the Requirements Budget and Ongoing Rate of Utilization for the Organization(s) It Serves

Effectively managing a business process involves having the authority and ability to derive an appropriate budget and control ongoing expenditures. Because each RAMP will be responsible for projecting estimates of the annual personnel security requirements for the component(s) it represents, it is both logical and practical that each RAMP also derive an associated annual budget and control its annual expenses. For WHS, which adjudicates access determinations for the White House and several Defense agencies, the WHS RAMP would not control the requirements budget for the components it represents but would serve as a requirements coordination, monitoring, and processing center.

As employers of personnel in sensitive positions, the components are both the source of requirements and the consumers of end products (PSIs and adjudicative decisions). Therefore, a RAMPs/DITTO model, with line-item personnel security budgets and authority, would create a true fee-for-service arrangement at a level of detail sufficient for each RAMP to track and control. Ongoing tracking and budgetary forecasts would be supported by information services supplied by DITTO, explained below.

The flow of field-initiated clearance requests through the RAMPs to PSI providers would normally be a seamless and uninterrupted stream of electronic documents over a secure network (supported by DITTO). As each electronic document/request is routed to an appropriate PSI provider, software at an applicable RAMP will:

1. Automatically check the clearance request for validity conditions, e.g., if the request pertains to a TS-PR for an Army officer, the software will confirm that the individual currently has an appropriate Army duty status.
2. Automatically assign an appropriate processing priority code.
3. Optionally assign an appropriate adjudicator to the case (see discussion of "Case Team" approach options, below).
4. Automatically increment the total case count and compare the current total to the expected total and available budget for the current time frame.

If the current total case-count is substantially different than the planned/budgeted cases for the current time frame, the software would send an alert to an appropriate RAMP manager. The RAMP will then work with the organization(s) it represents to determine what action is necessary. For example, if substantially more clearance requests than expected are coming in from the field, a RAMP may decide to temporarily delay forwarding low priority requests to PSI providers. Through such processing, each RAMP would be able to manage its budget and caseload commitments between the organization(s) it represents and the PSI providers.

Setting Processing Priorities for Personnel Requirements Within the Organization(s) It Serves

The Army, Navy, Air Force, DIA, NSA, JCS, and WHS have each consistently asserted that their personnel security needs are unique. Historically, this has been reflected in: [1] policy which gives each military service secretary legal authority over final security access determinations for that service, [2] their opposition to consolidating CAFs into a single adjudication facility, and [3] the reality that each DoD component is a separate organization that uses personnel security investigations and adjudications to serve its own organizational mission and responsibilities.

By staffing and managing each RAMP with component-specific experts, the RAMPs/DITTO model would better enable each of the military services, DIA, NSA, JCS, and WHS to determine and manage their own personnel security processing priorities. In current operations, DoD must pursue a component-wide consensus for DSS to apply a uniform set of processing priorities across all incoming PSI requests. In contrast, a RAMPs/DITTO model allows each major component organization to set and manage PSI priorities according to its own mission needs.

For example, if the Navy believes that its operations are best served by giving processing priority to SIOP-ESI cases (*Single Integrated Operational Plan-Extremely Sensitive Information*) over interim SCI cases, the Navy RAMP could assign relevant priority codes to Navy PSI requests en route to a PSI provider. If, however, the Army determines that it needs interim SCI cases to have top processing priority, the Army RAMP could prioritize Army PSI requests accordingly. Priority codes could be based on: [1] the four-tiered priority system that DSS currently applies to incoming PSI requests, [2] the fee-for-service model, whereby requests for faster processing equate to giving certain cases higher priority, which results in higher PSI charges to the requestor, or [3] new prioritization codes that combine or supplant other methods.

To ensure system-wide discipline in the assignment of priorities, e.g., to reduce the possibility of PSI providers being inundated because many RAMPs assign the highest priority to the majority of requests, each RAMP could be allowed an established annual quota for each level of priority. The quotas for each RAMP would be based on logical and historical needs, as well as the capacity and flexibility of PSI providers.

For issues that involve competing demands across RAMPs, each RAMP Director (or designate) would be empowered to negotiate with other RAMP Directors. For example, although each RAMP would be subject to an annual quota for the total number of PSI requests it can forward within each processing priority level, any RAMP could request from a PSI provider a temporarily higher quota to meet a current or anticipated surge in personnel security requests. The PSI provider(s) with the help of DITTO would assess whether a temporary surge in requests from one RAMP could be accommodated within normal system flexibility, e.g., by utilizing capacity resulting from RAMPs that are currently under-quota, or by estimating the potential for one or both PSI providers to temporarily increase contracted PSI services. If one or more RAMPs forward requests that cannot be accommodated through system flexibility, the RAMP Directors could request that DITTO supply them with the processing information, projections, and alternative processing options necessary for the RAMP Directors to negotiate among themselves for a total system solution. If the RAMP Directors cannot arrive at a mutually acceptable solution, they have an option to involve the *Personnel Security Oversight Committee* (PSOC, explained below).

Adjudicating Clearances by Means of an Internal Adjudication Facility

As described earlier, the military services, DIA, NSA, JCS, and WHS each maintains that their personnel security needs are distinctive, resulting in the current array of eight adjudication facilities. The RAMPs/DITTO model not only maintains this level of organizational control, but also increases the likelihood of efficient integration of planning, management, and communication at the organizational level by embedding each adjudication operation—e.g., as currently performed by a CAF—within an office structure (RAMP) that manages the entire organizational PSI obligation, strategy, and flow. Adjudication would proceed in much the same way as in the current system, although efficiency would be enhanced by incorporating next-generation information technology such as JPAS and DITTO. Additional benefits could also be realized through: [1] adoption of a "case team" approach (described below), and [2] development of an electronic Adjudicative Decision Support System (ADSS).

Adjudicative Decision Support System (ADSS). An automated ADSS system could offer significant benefits for improving personnel security clearance processing. An ADSS has the potential to aid adjudicators in reaching adjudicative decisions that are: [1] more objective , [2] more consistent and fair, and [3] accomplished in less time, thereby reducing costs, enhancing productivity, and improving customer satisfaction. As the name suggests, the ADSS would be designed to support adjudicators, not replace them.

A PERSEREC-sponsored report completed in 2001 (Sands, 2001, see Appendix C) suggests that it is feasible to develop an automated ADSS by combining expert knowledge available in the CAFs with software algorithms that integrate and process this knowledge according to "Case-based Reasoning" and related logic. For example, the ADSS could automatically generate an adjudicative recommendation for a case—based on adjudicative guidelines and best practices of the "whole person" approach—along with a brief summary outlining the decision logic and relevant ROI sections from which the recommendation was derived. The adjudicator could then review and accept the ADSS recommendation or set it aside in favor of his/her own review of all ROI information.

Assigning Adjudicators to PSI Cases During Investigation—the *Case Team* Approach

The efficacy of adjudication depends on the decisions and products of investigators, e.g., investigators' decisions on the amount of information to collect to address a potential issue, and then which information is necessary to include in the written product (ROI). The proposed RAMPs/DITTO Model, in which all clearance requests are managed and adjudicated by RAMPs, can be used to facilitate relevant communication and file sharing between investigators and adjudicators during the investigative process. The need for greater communication between investigators and adjudicators is based on the following observations.

- Investigators sometimes gather and forward information that is incomplete or not targeted to the adjudicative guidelines.
- Investigative reports with inadequate content or poor organization may undermine the timeliness and quality of the adjudicative review process and outcome.
- Adjudicators, faced with inadequate investigative reports, typically either: [a] send the file back for further investigation, or [b] adjudicate the case based on limited or ambiguous information.
- There is no standard procedure to allow an investigator or case analyst with a question to consult an adjudicator during the investigation process.
- There is no effective method for investigators, case analysts, and adjudicators, to share relevant databases and newly acquired information during the investigation process.

Although problems implicated by these observations are multifaceted, they may be partially remedied by enabling case related communication, collaboration, and file sharing during the investigative process, between investigators working on a case and the adjudicator who will eventually render the clearance decision for that case. We refer to this arrangement as the "Case Team" approach, which could function in the following way:

- An appropriate RAMP automatically assigns an adjudicator to potential issue cases (or, alternatively, every case) as cases are opened by a PSI provider. For example, based on issue-relevant information in the EPSQ, experienced adjudicators could be assigned to cases that are likely to involve difficult security issues.
- An investigative agency assigns a case analyst and investigator(s) to each case, forming a "case team" of the investigative staff and the assigned adjudicator.
- The case team members interact with each other as necessary via telephone, e-mail, and shared file access. For example, an investigator who is unsure about whether a particular foreign lead is important to interview could contact the assigned adjudicator, who would review available information on the case (e.g., the subject's EPSQ) and advise whether pursuit of the lead would be important to an adjudicative decision.
- The case team communications are supported by an end-to-end IT system into which case-relevant information is entered and viewed by any member of the case team.

If an investigator had no questions or issues to discuss with an assigned adjudicator, it is possible that no communication would occur between the two. Alternatively, it may be beneficial to have each adjudicator make a brief preliminary review of each assigned case file just prior to the case being forwarded from the PSI provider to the RAMP for adjudication. This would allow the adjudicator to spot potentially significant gaps in content prior to completion of the investigative phase and to request appropriate investigative attention. Although such a procedural policy would essentially eliminate the problem of incomplete files being returned to investigators, it would entail additional labor on the part of adjudicators.

An alternate form of implementing the case team approach would be to postpone the assignment of an adjudicator until key records, such as the national agency check and credit check, have been reviewed by a case analyst. This would allow for a more accurate determination of potential issue cases and, thus, a better assignment of appropriate adjudicators. Making assignments to issue cases only (as opposed to all cases) would also reduce the overall burden on adjudicators and focus case team efforts on cases of primary concern. The costs and benefits of such options should be investigated further.

Acting as the Single Point of Contact and Help Desk for the Organization(s) It Serves

By integrating and centralizing (within organizations) the management of PSI requirements, prioritization, case flow, and adjudication, each RAMP would be able to act as the main point of contact for the organization(s) it serves as well as OSD. This function would depend on the successful advent of integrated information technology such as the Joint Personnel Adjudication System and would be facilitated further by an overarching IT system such as DITTO (described below). Whereas DITTO-managed infrastructure would provide immediate and secure network access to any authorized manager or security officer to determine the processing status of any case submitted by their organization, RAMP staff would be available to personally answer more complex or sensitive questions.

For example, if an Army commander had a question regarding why the completion of one or more particular Army clearance cases was delayed, the commander could contact the Army

RAMP to inquire. Because the Army RAMP controls the flow of Army cases to PSI providers and then adjudicates the completed case files, Army RAMP staff would have direct access to relevant case processing details, as well as a direct commitment for serving in-house (Army) needs. If resolution requires contacting a PSI provider, the RAMP staff would initiate the contact because such staff would: [1] represent the Army entity that purchases PSI services and [2] understand both the big picture and detail of Army PSI requests. Consequently, an additional benefit of having RAMPs serve as the primary contacts between requestors in the field and PSI providers is that it should reduce and simplify the inquiries that PSI providers receive.

Finally, by serving as central sources of management and information on the personnel security plans, requirements, and operations of DoD components, the RAMPs would also function as central contacts for relevant informational requests by OSD, e.g., when OSD solicits information on how each military service plans to manage a current or anticipated surge in personnel security requirements.

Section Summary

In this section we laid out the organizational centerpiece of the proposed model and described how RAMPs would facilitate coordination among operational management, authority, resources, and accountability in the DoD personnel security system. The description has been at a general and conceptual level. Many operational details remain. The functioning of the RAMPs and other organizations in the proposed model will depend in part on the availability of end-to-end technology and the efficient flow and accessibility of electronic documents and information. The following section outlines how such end-to-end technological support can be achieved through development of a Defense Investigation Technology and Tracking Office.

Defense Investigation Technology and Tracking Office (DITTO)

> *Information, information processing, and communications networks are at the core of every military activity* (Director of Strategic Plans and Policy, 2000, P. 8).

Because the DoD personnel security system includes a variety of business processes and information exchanges, the system will function most effectively to the extent that a complete end-to-end technology model is designed to support information processing, program needs, and key business processes. In the RAMPs/DITTO model we propose to link DoD Components and industry, RAMPs, and PSI providers together with integrative information technology that supports current and foreseeable needs of the personnel security system. The IT system architecture would embrace and extend the most promising current initiatives, such as the Joint Personnel Adjudication System as well as planned developments, such as those associated with Automated Continuing Evaluation Systems. Because supporting technology has become an indispensable requirement for such systems, and because technological advances and opportunities occur at a quick pace, technological systems must also be managed—for current and future needs—by a dedicated staff. To meet this challenge, we propose the creation of a Defense Investigation Technology and Tracking Office. DITTO would be responsible for the following five functions, each of which is described in greater detail in the following sections.

1. Routing cases from customers in the field, through the appropriate RAMP, to the assigned PSI provider (DSS or OPM).
2. Collecting data on DoD personnel security system operations, developing metrics and statistics, and generating status reports.
3. Serving as the POC for the RAMPs, PSI providers, and OSD for monitoring categories of cases, issuing early warnings, and conducting "what if" analyses.
4. Serving as the system administrator and life-cycle resource planner for the complete IT system.
5. Managing IT system flexibility to meet competing demands across RAMPs or between PSI providers.

DITTO would not require a large staff. Although staffing requirements would be determined as part of a follow-up independent planning study on the architectural and functional specifications of the proposed IT system, we expect that DITTO could operate with a GS-15 level Director, several system administrators and computer technicians, and a few junior-level support staff. DITTO would strive to maximize the benefits of relevant IT programs that currently exist or are under development. For example, DITTO would coordinate closely with the ACES proposed Configuration Management Board (CMB), which includes representatives from the JPAS PMO, CAFs, Defense Manpower Data Center (DMDC), DSS, OPM, military counterintelligence, and C3I/S&IO. In addition, if the ACES CMB is established and proves effective, there may be benefits for including it as a subcommittee or advisory body to the PSOC. The role of DSS's Case Control Management System (CCMS) in DITTO will be explored as part of an independent planning study we recommend at the conclusion of this report. Although CCMS has recently improved, there is evidence that its basic architecture may not be suitable to the long-term needs of the personnel security system (TRW's In-Progress Review of DSS CCMS Remediation Activities, One Year Later: Final Report, 2000; Cox, Lt Col., 2001).

Routing Cases from the Field, through the Appropriate RAMP, to the Assigned PSI Provider (DSS or OPM)

The DITTO/RAMPs model is based on a personnel security system that functions primarily on electronic information exchanges between interoperable databases that link field offices (requesters), RAMPs, and PSI providers. This type of paperless network would enable a Facility Security Officer (FSO or equivalent) in the field to initiate an electronic request for a PSI, e.g., for an initial TS request, the FSO would complete an online field authorization form and attach the subject's completed[9] Electronic Personnel Security Questionnaire (standardized EPSQ, EQIP, or equivalent), and digitized fingerprints. DSS and OPM currently have several initiatives that would support a paperless front-end, although there is no final consensus on which PSQ standard (EPSQ or EQIP) should be adopted system-wide.

[9] At the time a subject completes an EPSQ, verification software would automatically check whether information contained in the EPSQ was ostensibly complete and consistent, e.g., that all required fields had been completed and that no logical inconsistencies or errors, such as six-character SSNs or impossible date ranges, had been entered. An acceptable verification code would be required for submission of a completed EPSQ by an authorized field representative.

The information contained in the field authorization form and EPSQ would automatically be compared against RAMP personnel databases to ensure: [1] that the subject's current position (e.g., based on the position's Special Access Requirement code) and personnel status (e.g., active personnel not slated in the short term for retirement or transfer to a position that would obviate the need for a PSI) were consistent with the requested access level[10], and [2] that the requesting official was authorized to initiate such a request. Electronic requests that were inappropriate, unauthorized, or incomplete would not proceed to a RAMP but, instead, would automatically cause a system notification describing the request suspension and necessary corrections to appear on the requester's terminal. A simultaneous notice would also be sent to a DITTO quality control database for use in understanding local and system-wide usability patterns, such as characteristics of the software that are difficult to use and could be improved, and to assess whether the suspended submission was an attempt to initiate a fraudulent PSI request.

For valid requests, the DITTO system would forward the electronic request, EPSQ, and attachments from the field to a PSI provider, e.g., DSS or OPM. Network software would be programmed to route cases according to a PSOC-preferred allocation procedure, such as: [1] a provider-specific pre-negotiated allocation, e.g., all SSBI-PRs go to DSS, [2] a dynamic allocation, e.g., to whichever PSI provider had the most available investigative personnel, [3] a free-market allocation, e.g., to whichever PSI provider is currently preferred by the requestor, or [4] a hybrid allocation that includes two or more of these methods (as discussed below, we propose an allocation method that combines a guaranteed base workload with some degree of flexibility). As an end-to-end IT integrator, a DITTO-managed IT network would also facilitate data transfers and notifications from the PSI providers back to the RAMPs, and ultimately to the original requestor, e.g., through database and notification functions in JPAS.

As described above, each requestor would be affiliated with a designated RAMP, e.g., all Army PSI requests would be managed by the Army RAMP. The networked system managed by DITTO would enable each RAMP to monitor its own flow of electronic PSI requests from the field to PSI providers, with the prerogative to modify a predefined priority code and/or assign an appropriate adjudicator to each PSI request. A RAMP would interrupt the flow of PSI requests only under extreme circumstances, such as controlling the flow of requests during the last month of a fiscal year in response to a nearly exhausted PSI budget.

Collecting Data on DoD Personnel Security System Operations, Developing Metrics and Statistics, and Generating Status Reports

Decision makers and managers need accurate and timely performance information. DITTO's responsibility for managing the personnel security system computer network, databases, and associated technology would include generating statistics and reports on system-wide performance. Although standard period reports could be sent on a regular basis to OSD, RAMP Directors, and other appropriate stakeholders, reporting tools and templates also could be used to calculate performance metrics at any time for any prescribed period. This kind of access and report generation would be similar to currently available online tools for dynamically

[10] The Air Force is currently integrating personnel and manpower databases for its personnel security requirements model that would allow for the proposed DITTO check based on the subject's SAR code and employment status.

creating customized displays of the performance of the stock market, user-defined portfolios, or individual stocks, for a given time period.

For example, personnel security system reports could include performance profiles summarizing and comparing *metrics*, e.g., submitted PSI requests, actual completion times, access denials and revocations, and current levels of fee-for-service payments, with *standards*, e.g., annual PSI budgets, planned annual PSI requirements, and target PSI completion times. Standards for annual budgets and requirements would be based on Planning, Programming, and Budgeting System (PPBS) guidance. Standards for completion times would be based on timeliness thresholds expressed in the Draft DoD Strategic Plan for Personnel Security. Because DITTO would have access to military accessions and classification data each month, it could report on imminent PSI decreases or surges (e.g., see "early warning" example below). Finally, as JPAS and ACES become fully operational, DITTO would be able to integrate data from those systems into reports of performance metrics and standards.

Serving as the POC for the RAMPs, PSI Providers, and OSD for Monitoring Categories of Cases, Issuing Early Warnings, and Conducting "What If" Analyses

Decision makers and managers need a responsible "go to" office for questions about personnel security trends and forecasts. Although an integrated computer network with customizable reporting tools would allow authorized users to quickly track the history and current status of a particular PSI request or group of cases, it is also imperative that users, PSI providers, and supervisors have a clear POC with staff who are knowledgeable and capable of handling complex data and technology related issues. Thus, in situations when automated computer tools and customizable report templates do not suffice, it is important that responsible DITTO staff be available to answer questions and service special IT requests.

Just as electricity power grid managers monitor system-wide performance in order to warn local supervisors and avert imminent difficulties, DITTO would be responsible for issuing "early warning" notices when the flow of one or more categories of PSI requests is likely to strain an important part of the personnel security system.

Example of an Early Warning Scenario and Response. After a RAMPs/DITTO model has been operating for a year, DITTO would be able to derive estimates of workflow and capacity throughout the personnel security system in terms of standard "PSI units." Equating different PSI activities in terms of standard PSI units is useful for estimating workload and budget requirements. For the sake of this example, a National Agency Check with Local Agency and Credit Checks (NACLC) will be equal to one PSI unit, a TS-PR is equal to five PSI units, and other PSI products are weighted accordingly. As a further assumption, we can specify that DSS does all DoD accessions and PRs, and has determined that it can handle 10,000 PSI units per month, with flexibility to service up to an additional 1,000 PSI units/month while maintaining completion time standards. If, through DITTO's monitoring of monthly accessions data and JPAS's log of upcoming SSBI-PRs, it determines that there are likely to be substantially more than 11,000 PSI units for DSS in the coming months DITTO could issue an "early warning" notice to the RAMPs, PSI providers, and OSD. The notice would include details of the prediction and several management options, e.g., temporarily routing workload from DSS to

OPM, reprioritizing specific types of PSI requests, or temporarily resourcing additional PSI contractor support. Each proposed management option would include estimates of the likely effects on case completion times and PSI costs. Policy makers would establish which types of remedies, e.g., involving SCI cases or total costs greater than a particular amount, would require specific approval by RAMP Directors, PSI providers, or the PSOC.

Whereas the example above outlines how DITTO could use actual data on workload changes to help predict and ameliorate impending strain in the personnel security system, DITTO could also use system modeling tools and presumptive test data to explore "what if" scenarios related, for example, to understanding the likely consequences of proposed policy changes, prolonged increases in PSI requirements, or organizational restructuring.

The Options project explored the feasibility of developing modeling tools. As summarized in Appendix D and detailed in a full report entitled "Development of a Computerized Simulation Model of the Personnel Security Clearance Process for the Department of Defense: A Feasibility Study" (Sands, 2001), developing modeling tools is feasible, and the product is likely to be very useful. Specifically, developing such capabilities offers the promise of providing a powerful and flexible decision support tool not only to ASD(C3I) decision makers, but also to other DOD agencies (e.g., the Defense Security Service) and government agencies outside of DOD (e.g., the Office of Personnel Management). The model would be useful to managers responsible for planning, policy, operations, evaluation, and costs of personnel security clearances. Example uses of the model include:

1. Simulating changes to the current personnel security processing system (e.g., alternative resource investment scenarios).
2. Examining the predicted consequences of implementing alternative policies, both in terms of case backlogs and costs.
3. Evaluating the tradeoffs between case processing strategies in terms of benefits and costs.
4. Identifying those strategies that offer the greatest net benefits.

Thus, as the office responsible for data and technology integration for the personnel security system, DITTO would be able to serve as the POC for the RAMPs, PSI providers, and OSD for special services, such as complex data assessments, preemptive operational alerts, and modeling "what if" system scenarios.

Serving as the System Administrator and Life-Cycle Resource Planner for the Complete IT System

In the RAMPs/DITTO model, information technology serves the needs of the personnel security system. Because personnel security and IT systems are affected by technological developments and governmental changes over time, proactive IT management is essential for ensuring ongoing operational success. DITTO—with input from the RAMPs, PSI providers, OSD, and the PSOC as necessary—would manage IT administration and IT planning for the personnel security system. Responsibilities would include:

1. Managing the current operational status and maintenance of personnel security computing technology, databases, and information systems.
2. Planning for short-term and long-term technological change and IT life-cycle options, such as assessing cost effectiveness considerations for when parts of the IT infrastructure (hardware and software) should be upgraded to avoid diminished performance.
3. Managing personnel security IT standards, e.g., regarding database dictionaries, use of middleware, electronic document formats, use of COTS hardware and software, compatibility and usability of system interfaces, Internet and NIPRNET accessibility, and interoperability with other DoD authorized systems.
4. Managing IT security, including maintaining or exceeding DoD and government-wide standards for security, privacy protection, data backup, and ongoing risk assessment.

Thus, with respect to technology, DITTO would take the lead in managing, maintaining, coordinating, and planning for services that support the personnel security system.

Managing IT System Flexibility to Meet Competing Demands across RAMPs or Between PSI Providers

As described in the "early warning" scenario above, variation in month-to-month PSI requests and operational conditions may occasionally stress the capabilities of the personnel security system. For managing these stresses, it will be important to clearly specify which types of remedies DITTO is authorized to implement without seeking external approval. System efficiency will be enhanced to the extent that DITTO can immediately implement a wide range of remedies that have been pre-approved by the principal stakeholders, i.e., the RAMPs, PSI providers, and PSOC. Pre-approved remedies would be based on case types and maximums regarding additional PSI costs and processing time. For example, relevant stakeholders could agree that DITTO would reroute military accessions to either PSI provider, where the estimated PSI costs for those cases would not increase more than 5% over the established budget, in order to maximize efficient load balancing across the system. Because each RAMP would use fee-for-service (see description, below) to pay only for PSI services actually rendered, fiscal equity would be maintained.

Development Issues

DITTO, the office and system-wide infrastructure, would be essential for implementing the RAMPs/DITTO model. For example, technology-based resources, information services, and DITTO support would be necessary: [1] for the RAMPs to effectively administer personnel security requirements, and [2] for OSD and the PSOC to have detailed, accurate, and timely information on which to base oversight deliberations. Furthermore, DITTO-related infrastructure, such as designs, hardware, systems integration, programming, testing, would likely be the most expensive aspect of developing the RAMPs/DITTO model. Consequently, DITTO represents an important and expensive part of the RAMPs/DITTO vision.

Although a vision is necessary, it is not sufficient for success. Sweeping visions for tying together many databases and computers have been known to fail under the weight of their own ambition (e.g., see Rosenthal, Manola, Renner, 2000, for a discussion of why many IT plans fail). Thus, DITTO must be developed: [1] with regular participation of the principal users and stakeholders in the RAMPs/DITTO model, such as the military services, CAFs, relevant defense agencies, DSS, OPM, USIS, DMDC, and C3I/S&IO, [2] in concert with relevant systems currently under development (e.g., JPAS, ACES, Air Force requirements model), [3] in accord with government and industry-wide best practices in developing metadata codes and Extensible Markup Language (XML) to facilitate data exchanges between disparate systems (e.g., U.S. GAO, 2002; Duval et al, 2002), [4] to be consistent with DoD-wide CIO strategic initiatives for information systems as developed by C3I and the Chief Information Officers Council (e.g., Yoemans, 2000), and [5] in accordance with DoD guidelines for pursuing IT developments of this kind; see for example, Raines Rules (Office of Management and Budget, 1996), Clinger-Cohen Act (Clinger-Cohen Act of 1996), and Major Automated Information System Acquisition Programs (MAISAP, DoD 5000.2R, 2001). We expect that DITTO would be run by a Program Management Office (PMO), which would be responsible for submitting an annual operating budget request. Candidate PMOs would include the Air Force, which is currently managing JPAS.

Section Summary

In this section we outlined the principal functions and benefits of DITTO, which is the office and system-wide infrastructure that facilitates the RAMPs/DITTO model of personnel security. Fundamentally, DITTO focuses on IT integration, interoperability, and special services to support the work of the personnel security system.

> Achieving and sustaining interoperability is a DoD enterprise-wide responsibility that must be woven into the thread of organizational roles, responsibilities, processes, and resourcing. (DoD Instruction 4630.8, 2001).

For integration and interoperability to succeed, technological plans must be developed in concert with program requirements, applicable policy, and the business processes of affected organizations throughout the personnel security system and DoD.

Personnel Security Investigation Providers

Although personnel security investigative services could be supplied by one, two, or several providers without altering the basic architecture of the RAMPs/DITTO model, we present a functional outline with two PSI providers (such as DSS and OPM) in the proposed model. Five attributes of this model are each described in greater detail in the following sections.

1. Two PSI providers (such as DSS and OPM) to enhance system flexibility and reduce the risk of system failure.
2. Each PSI provider has a guaranteed base workload, reviewed semiannually by the PSOC.
3. Each RAMP uses “fee for service” to pay for the provision of PSIs.
4. PSI providers address inquiries from RAMPs rather than directly from requesters in the field.
5. Investigators may work with adjudicators as a case team during the course of a PSI.

Two PSI Providers (such as DSS and OPM) to Enhance System Flexibility and Reduce the Risk of System Failure

Since the late 1990s DoD has often had to rely on OPM to offset a PSI backlog and to cope with processing difficulties experienced by DSS. This history demonstrates the value of a personnel security system with two or more PSI providers for reducing dependency on any single provider and decreasing the risk of a single point of system failure.

For the future, it will also be wise to ensure that at least one PSI provider is a DoD agency. Non-DoD government agencies may be less responsive to DoD needs and directives. Furthermore, an over-reliance on a single commercial PSI provider increases the risk of dependency on a monopoly that is more beholden to shareholder's interests than to DoD.

Are PSI Services Inherently Governmental? Current pressure across DoD to outsource functions that are not inherently governmental raises an important consideration regarding whether PSI services should fall under such a designation.

OMB Circular No. A-76, (OMB, 1999) SUBJECT: *Performance of Commercial Activities* specifies the following definition.

> An *inherently Governmental function* is a function which is so intimately related to the public interest as to mandate performance by Government employees. Consistent with the definitions provided in the Federal Activities Inventory Reform Act of 1998 and OFPP Policy Letter 92-1 (U.S. OMB, 1992), these functions include those activities which require either the exercise of discretion in applying Government authority or the use of value judgment in making decisions for the Government. … [such as]:
>
> (1) The *act of governing*; i.e., the discretionary exercise of Government authority. Examples include criminal investigations, prosecutions and other judicial functions; management of Government programs requiring value judgments, as in direction of the national defense; management and direction of the Armed Services; activities performed exclusively by military personnel who are subject to deployment in a combat, combat support or combat service support role; conduct of foreign relations; selection of program priorities; direction of Federal employees; regulation of the use of space, oceans, navigable rivers and other natural resources; direction of intelligence and counter-intelligence operations; and regulation of industry and commerce, including food and drugs.

Do personnel security investigators use "value judgment in making decisions for the Government"? The answer is "yes." Investigators are required to determine whether the subject of a personnel security investigation has engaged in behavior that may relate to the subject's loyalty, trustworthiness, or suitability for accessing sensitive information. The majority of these subjects are military personnel who may be deployed in combat or combat support roles. Although government adjudicators render most final decisions on whether subjects should be granted a clearance for initial or continued access, for SSBI cases it is the investigative staff who make substantial early decisions regarding (e.g., for Top Secret, SCI, and SAP applications): [1]

who among the subject's associates, neighbors, and coworkers is most important to interview, [2] which information is likely to be important, with respect to adjudicative significance, [3] when parts of an investigation should be expanded with supplementary interviews, additional records checks, or further inquiries, [4] whether surfaced information appears to relate to counterintelligence concerns and should be reported to a CI office, and [5] what information should be included or highlighted in the report of investigation. The ROI is the primary document adjudicators use to evaluate subjects and determine their fitness for access to sensitive information and environments. Thus, personnel security investigators make numerous and substantial value judgments in determining what information is appropriate to forward to adjudicators. Poor investigative judgment can compromise the efficacy of adjudication and increase risk in areas of public trust and national security[11]. As highlighted by Congressman Christopher Shays in his opening remarks for a Defense Security Service oversight hearing:

> The Department of Defense relies on personnel security investigations to determine whether individuals should have access to classified information. It is a process critical to safeguarding the national security. (Management challenges confronting the Defense Security Service, 2000)

The design and function of the RAMPs/DITTO model is flexible for any proportion of federal versus contract investigators. Nevertheless, we recognize that this is a current topic of debate and proffer our view that personnel security investigation, at least with respect to Top Secret, SCI, and SAP cases, is intimately related to the public interest and constitutes an inherently governmental function.

This logic further supports the benefits of including at least one DoD agency (such as DSS) as a PSI provider in the RAMPs/DITTO model. Specifically, this would allow the DoD agency to concentrate on inherently governmental investigations that involve SSBIs and SSBI-PRs, such as for Top Secret, SCI, and SAP, whereas the second agency, which could be a non-DoD government agency such as OPM or a private contractor such as Omniplex, could concentrate on other investigations, such as military accessions, Secret, Confidential, and checks for sensitive but unclassified access, i.e., cases that do not require a SSBI.

[11] Although we base our logic and conclusion regarding the outsourcing of PSI services on the 1999 revised OMB circular cited above, we also recognize potentially conflicting language contained in earlier documents, e.g., Policy Letter 92-1, Sep. 23, 1992 and Public Law 105-270, Oct. 19, 1998 *Federal Activities Inventory Reform Act of 1998* (FAIR Act). The FAIR Act states in Sec 5 Definitions, (2) Inherently Governmental Functions, (C) Functions Excluded: "The term [inherently governmental] does not normally include (i) gathering information for or providing advice, opinions, recommendations, or ideas to Federal Government officials." In this definition of excluded functions, the phrase "does not normally include" is the key to reconciling language in the 1999 OMB Circular and earlier documents. Specifically, such language implies that "gathering information" represents a continuum of behaviors ranging from those that should "normally" be designated as inherently governmental to those that should not. For example, information gathering that is inherently governmental would normally require substantial individual judgment and relate intimately to public trust or national security concerns, e.g. clandestine services, whereas noninherently governmental information gathering would normally require minimal individual discretion and have little direct relation to public trust or national security, e.g., bibliographic searches on nonmilitary topics. Based on the requirements of personnel security investigators (outlined above), we assert that PSI services for SSBIs and SSBI-PRs—at least with respect to Top Secret, SCI, and SAP cases—require a sufficient level of individual judgment bearing on national security and public trust as to be designated inherently governmental.

Each PSI Provider has a Guaranteed Base Workload, Reviewed Semiannually by the PSOC

Organizations are best able to provide services when they know the approximate volume and timing of forthcoming work. For PSI providers, this foreknowledge helps to ensure that staffing levels and contractor support will be sufficient to deliver requested PSI services and quality products on time. Because the RAMPs' responsibilities would include projecting annual personnel security requirements for submission to the DoD budget process, it would be possible to allocate a large portion of those requirements as initial workload bases between the PSI providers, along with a provisional division of the remaining requirements. The guaranteed workload would help PSI providers budget for their organizations, whereas the remaining provisional workload would represent the possibility of reallocating work, e.g., up to 10% of the guaranteed base, on a quarterly or monthly basis when such "load balancing" is deemed necessary by DITTO and/or the RAMPs to maintain overall efficiency or to manage exigencies.

PSI provider performance would be reviewed at least semiannually by the PSOC using standardized metrics for PSI costs, timeliness, and quality.[12] Based on PSI performance reviews along with other relevant considerations, the PSOC would determine the necessity for modifying the overall volume or case mix of future PSI workload assignments for the following year between the PSI providers. Continuous poor PSI performance could result in substantial reductions in workload and income for a PSI provider. These reviews would thus provide an opportunity for performance feedback and guidance to PSI providers as well as an incentive for them to maintain acceptable performance levels.

Each RAMP Uses "Fee for Service" to Pay for the Provision of PSIs

The RAMPs/DITTO model supports OSD's current fee-for-service (FFS) initiative, although further research would be needed on how (or if) FFS should be applied to an industry RAMP. FFS typically improves system efficiency by motivating requestors to purchase necessary services only, and there is some speculation that instituting FFS at OPM helped that organization to improve PSI quality and turnaround time (Joint Security Commission, 1994).

Although FFS should generally improve the efficiency of the personnel security system, current debates highlight the challenges of applying FFS to defense contractors (see Appendix E). Such debates should be considered in subsequent research focused on specifying the detailed processes for how the industry RAMP would best fulfill its mission.

For the military services and DoD agencies, FFS would foster greater budgetary discipline across organizational processes for generating program needs and PSI requirements. As described in the RAMPs section (above), this discipline would be coordinated and managed by each RAMP. For PSI providers, there would be a direct connection between services provided

[12] Standards for PSI timeliness appear in the Draft DoD Strategic Plan for Personnel Security. Standards for quality are currently being developed through efforts at PERSEREC, DSS and elsewhere, and are likely to include measures regarding scope (i.e., completing all investigative activities specified by DCID 6/4), coverage of concerns and mitigating factors articulated in the adjudicative guidelines, and utility as assessed by adjudication facilities.

and income. For OSD and the DoD comptroller, the resulting effects should improve how PSI budgets are justified and allocated, and facilitate the accounting of ongoing resource utilization.

PSI Providers Address Inquiries from RAMPs Rather than Directly from Requestors in the Field

Just as each RAMP will act as the POC for inquiries from PSI requestors it serves, the PSI providers will act as the POCs for the RAMPs. In most cases, PSI status information should be available online in databases managed by DITTO, thus obviating the need for security managers and FSOs to contact PSI providers directly. For questions and complaints that cannot be satisfied through online access to databases, RAMPs' staff would contact the appropriate PSI provider. This would simplify and reduce the number of inquiries to the PSI providers and help to maintain the role of the RAMPs as the coordinating organizations in the personnel security system.

Investigators May Work with Adjudicators as a Case Team During the Course of a PSI

As described in the RAMPs section (above), there are benefits for enabling case-related communication, collaboration, and file sharing during the investigative phase between investigators working on a case and the adjudicator who will eventually render the clearance decision for that case. With guidelines to ensure that investigators maintain proper control over the investigative process and that adjudicators are not inundated with inappropriate questions, such a "case team" approach could improve the overall quality and efficiency of the personnel security system.

Section Summary

In this section we described the benefits of a personnel security system with two PSI providers, one of which is a DoD agency. Although DSS and OPM were used as examples of PSI providers, the RAMPs/DITTO model includes "PSI Providers" in terms of organizational roles, with some operational examples, i.e., the model is not based on a presumption that either DSS or OPM is ideal to fill such a role. We also described the benefits of instituting the fee-for-service initiative and employing RAMPs as the primary liaisons between RAMPs' constituents in the field and PSI providers. Although we mentioned again the "case team" approach, we note that this does not represent a requirement of the RAMPs/DITTO model, but rather an innovative operational alternative for consideration.

Oversight

Effective oversight and clear lines of accountability for policy and operations are essential for a well functioning personnel security system. OSD/C3I develops and coordinates relevant policy. However, system-wide operational oversight and performance accountability are not clearly vested in any single office or group. The GAO has focused attention on this concern as a DoD-wide issue.

> DoD has not routinely established accountability for performance to specific organizations or individuals that have sufficient authority to accomplish desired goals. (U.S. General Accounting Office, 2001, P. 8)

Congressional hearings have specifically noted the concern for the personnel security program. The following is an exchange between U.S. Representative Christopher Shays and former Assistant Secretary of Defense (ASD/C3I) Arthur Money regarding operational oversight for the DoD personnel security program (Defense Security Service, 2001b.):

> Shays: But again, let me ask you. Who has overall command of that?…Is there one person?
> Money: The Secretary of Defense is the one person.
> Shays: No, that's not good. That's not good. There's no one person that is following this, is taking charge?

As Mr. Shays suggests, it is unreasonable to expect the Secretary of Defense to actively oversee personnel security operations. The solution we propose is for C3I to constitute a Personnel Security Oversight Committee (PSOC) that represents the principal stakeholders across the personnel security system and, with their input, to craft an appropriate set of goals, responsibilities, and schedules for the PSOC and one or more subcommittees. Three elements, each described in sections below, constitute an outline for the PSOC.

1. Include representatives of the principal stakeholders, at a level sufficient to oversee Directors of the RAMPs, DITTO, and PSI providers.
2. Oversee DoD personnel security policy and operations.
3. Include a technical subcommittee as support for assessing and implementing technical solutions.

Include Representatives of the Principal Stakeholders, at a Level Sufficient to Oversee Directors of the RAMPs, DITTO, and PSI Providers

Members of the PSOC need to represent the principal stakeholders of the DoD personnel security system, i.e., the military services, OSD/C3I, and the intelligence community, and have the authority to direct personnel security policy and resources for organizations under their purview. Because OSD/C3I is responsible for DoD personnel security policy, an SES-level C3I official, such as the DASD C3I/SI&O, should chair the PSOC. Thus, individuals in the following five positions would be appropriate members of the PSOC.

1. Deputy Assistant Secretary of Defense, OASD/C3I/SI&O [PSOC Chairperson]
2. Assistant Secretary of the Army, Military Personnel Management
3. Administrative Assistant to the Under Secretary of the Navy
4. Administrative Assistant to the Secretary of the Air Force
5. A senior CIFA official

Oversee DoD Personnel Security Policy and Operations

The mandate of the PSOC is to oversee system-wide issues regarding DoD personnel security policy, operations, and outcomes. The PSOC would not be expected to micromanage operations. For the personnel security system to be effective, there must be clear lines of management and accountability at every level of participating organizations. However, there must also be an individual or governing body, such as the PSOC, that pays attention to and takes responsibility for system-wide performance. In practice, a technical subcommittee (described below) and other subcommittees as necessary—for example, a Policy and Strategic Planning Subcommittee[13]—would manage the details of system-wide oversight and prepare briefings on issues that require PSOC approval or attention. Thus, the primary activity of the PSOC will be to review status reports and briefings from subcommittees and to make management decisions based on briefed options. For example, if a PSI provider consistently failed to meet PSI completion time standards, the PSOC would be briefed by a subcommittee or appropriate research organization on options for rectifying the problem. The PSOC would select an appropriate option and sanction resources and policy memos as necessary or, alternatively, direct that further options be explored.

The PSOC would submit concise biannual status reports to the ASD/C3I, who would forward such reports, with additional information as necessary, to the DepSecDef.

PSOC decisions would be guided by the ten goals articulated in the draft DoD Strategic Plan for Personnel Security (2000):

Goal 1. Policy and oversight: effective and timely policy development and implementation, with active oversight by senior management.
Goal 2. Resources: resource allocation that is integrated with personnel security policy development and implementation.
Goal 3. Clearance requirements: predictable clearance requirements that are tied directly to position risk factors.
Goal 4. Investigations: personnel security investigations that are timely, high quality, consistent, and in accordance with all applicable standards.
Goal 5. Adjudications: adjudications that are timely, high quality, and in accordance with all applicable standards.
Goal 6. Continuing evaluation: a proactive continuing evaluation program.
Goal 7. Security awareness: effective security awareness and compliance at all levels within DoD.
Goal 8. Sensitive but unclassified information and environments: effective risk management of individuals with sensitive duties but no access to classified information, especially information technology personnel with access to high risk data and information systems.
Goal 9. Training and professional development: comprehensive recruitment, training, education, and professional development of security personnel, along with appropriate infrastructure.

[13] A Personnel Security Strategic Plan Implementation Committee has already been formed and has met twice in 2001.

Goal 10. Research: a personnel security research capability in support of DoD and national security strategic priorities.

The PSOC would pay closest attention to four objectives specified under Goal 1:

1.1: Compatibility between the DoD and DCI Personnel Security Strategic Plans.
1.2: Consistent and effective policy implementation.
1.3: Programs and proposals that include measures and the means to evaluate and monitor program effectiveness.
1.4: Policy formulation that is supported by research wherever feasible.

Include a Technical Subcommittee as Support for Assessing and Implementing Technical Solutions

A technical subcommittee comprised of RAMP Directors, the DITTO Director, and Directors of each organization providing PSI services would oversee most system-wide technical and operational issues. For example, whereas DITTO would take the lead on researching and recommending system-wide IT upgrade options, RAMP and PSI Directors would need to have an opportunity to discuss consequences of each option for their organization's budget and operation. Similarly, this technical subcommittee would consider proposals for modifying document or database standards that could affect information flow among different parts of the personnel security system. Any issues that could not be resolved within the technical subcommittee, e.g., subcommittee disagreement regarding a proposed operational modification affecting clearance reciprocity, would be briefed to the PSOC for a final decision. An important goal of this subcommittee will be to coordinate with relevant IT programs, e.g., coordinating with the proposed ACES CMB, so that oversight across JPAS, ACES, and other IT resources is seamless and effective.

Section Summary

In this section we outlined the core functions, goals, and composition of the PSOC, a committee structured to provide system-wide operational oversight and performance accountability for DoD personnel security. PSOC members would be SES-level administrators from the military services, intelligence community, and OSD/C3I, i.e., principal stakeholders in the personnel security system. PSOC subcommittees would include directors of RAMPs, DITTO, and PSI providers, as well as personnel security policy representatives. These subcommittees would manage and coordinate most system-wide issues, such as performance assessments, IT management, and problem resolutions, and would brief the PSOC periodically on system status and on matters that require PSOC decisions. Thus, the PSOC and its subcommittees would ensure system-wide direction, coordination, and oversight for DoD personnel security, and provide a single source of accountability.

Process Flow in the RAMPs/DITTO Model

In this section we employ a hypothetical scenario to illustrate several important business processes in the RAMPs/DITTO model.

Managing a Surge in Personnel Security Requirements

Figure 3 illustrates how organizations in the RAMPs/DITTO model would function in response to a surge in personnel security requirements. The example, based on responses to a hypothetical military operation named "Safe Sands," illustrates the coordination of evaluation, strategy generation, resource planning, policy development, and execution across the proposed DoD personnel security system.

The example depicted in Figure 3 begins with a request from the ASD/C3I to the PSOC to support an imminent surge in DoD personnel security requirements. Handling of this request can be summarized by the following four steps.

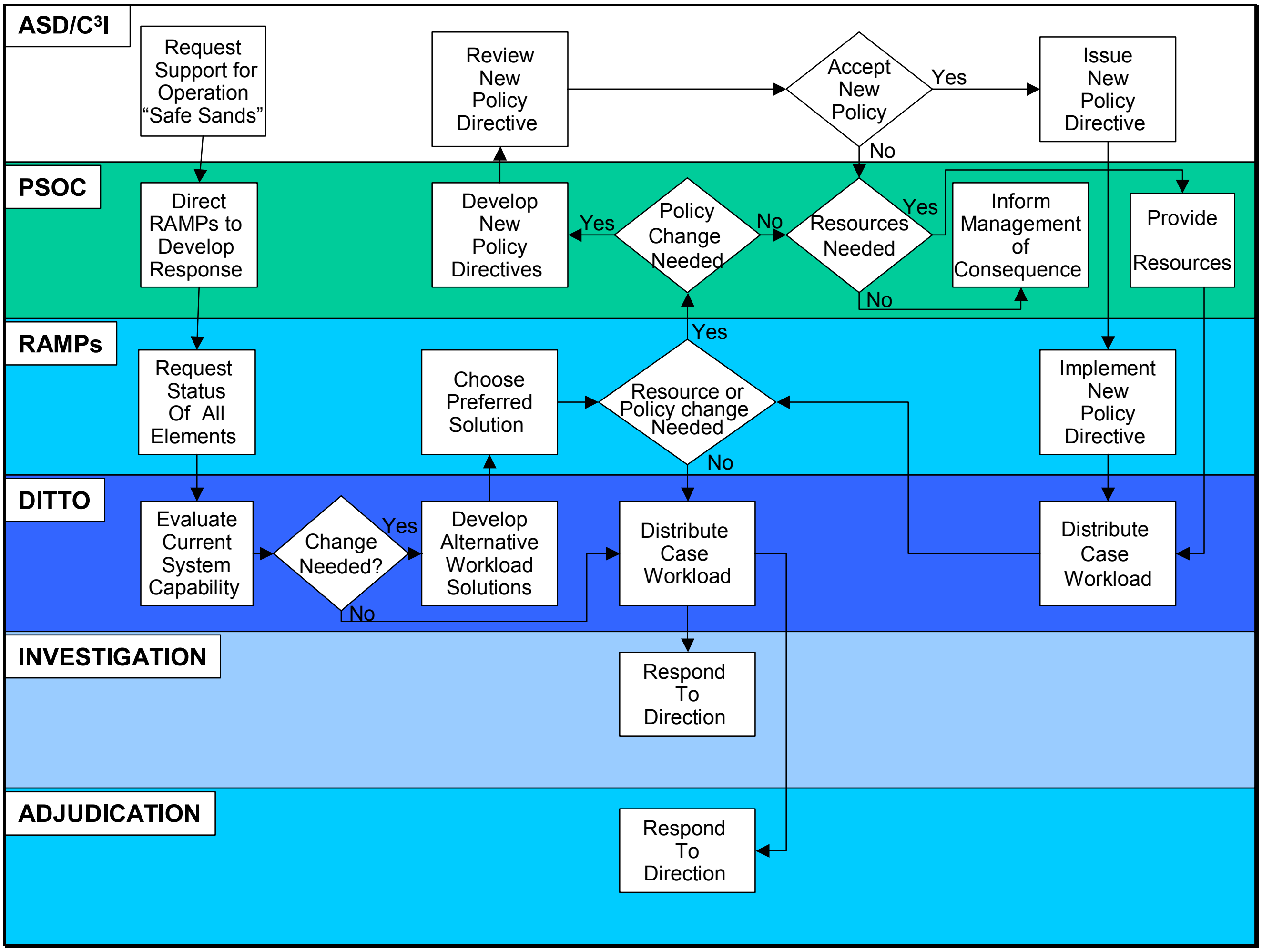

ASD/C³I
Request Support for Operation "Safe Sands"
Review New Policy Directive
Accept New Policy
Yes
No
Issue New Policy Directive
PSOC
Direct RAMPs to Develop Response
Develop New Policy Directives
Yes
Policy Change Needed
No
Resources Needed
Yes
No
Inform Management of Consequence
Provide Resources
RAMPs
Request Status Of All Elements
Choose Preferred Solution
Yes
Resource or Policy change Needed
No
Implement New Policy Directive
DITTO
Evaluate Current System Capability
Change Needed?
Yes
No
Develop Alternative Workload Solutions
Distribute Case Workload
Distribute Case Workload
INVESTIGATION
Respond To Direction
ADJUDICATION
Respond To Direction

Figure 3 Organizational Process Flow in the RAMPs/DITTO Model.

1. The PSOC technical subcommittee would recognize that the first step in responding would be to estimate the likely size of the surge in requirements and the personnel security system's ability to accommodate it. Thus, the subcommittee would task the RAMPs to conduct an evaluation of expected requirements and solutions.

2. Each RAMP would feed its requirements estimations to DITTO, which would evaluate overall system and IT capability to handle the surge, e.g., by temporarily reprioritizing incoming requirements. If DITTO could accommodate the surge within normal system processing limits, i.e., by using modest system adjustments that it typically controls, then DITTO would allocate IT workload accordingly. Otherwise DITTO would develop alternative workload solutions and, optionally (not shown in Figure 3), request input from PSI providers and adjudication facility managers regarding their ability to increase available labor. DITTO would then forward proposed solutions to the RAMPs.

3. RAMP directors would then agree on a preferred solution or, in the case of disagreement (not shown in Figure 3), request PSOC intervention. A RAMPs-preferred solution that does not require a system-wide policy change or substantial additional resources would be implemented immediately. Otherwise, a request would be forwarded to a PSOC subcommittee for policy development and/or consideration of supplemental resources. Subcommittee recommendations would be briefed to the PSOC for approval.

4. Any policy or resource request that required approval authority above that held by the PSOC would be forwarded to the ASD/C3I for review and signature.

This example demonstrates how organizations in the RAMPs/DITTO model would accommodate a surge in personnel security requirements by executing effective processes characterized by coordinated responsibility and decision-making under a single umbrella of performance and policy oversight. The RAMPs/DITTO design appears capable of handling either normal or challenging personnel security requirements and, as described in an earlier section, is able to accommodate promising new initiatives such as JPAS, ACES, and phased PRs.

Section Summary

In this section we explored how organizations in the RAMPs/DITTO model would work together in response to an expected surge in personnel security requirements. The example highlighted specific processes as well as the overall effective coordination of responsibilities and decision-making throughout the system. As described in an earlier section, the RAMPs/DITTO model would also be robust with respect to three forthcoming personnel security initiatives—JPAS, phased PR investigations, and ACES—that would each have implications for decision-making and process flow within the personnel security system and, collectively, would be coordinated through DITTO. Consequently, the RAMPs/DITTO model should serve as a coordinating force that both integrates and extends the potential benefits of these personnel security initiatives.

Summary

The objective of the Options project was to consider prior studies of DoD's personnel security program, relevant program initiatives and strategic goals, organizational principles that enhance effectiveness, and the role of information technology in designing a more coherent and effective personnel security system. We believe that the resulting RAMPs/DITTO model combines current system strengths, recent innovations such as JPAS and ACES, broader and more effective use of information technology, and coordinated operational oversight to best serve DoD's needs in the coming decade and beyond.

The model depends on the functions of and interactions among several organizations: the RAMPs, DITTO, and PSOC. With respect to RAMPs, we find both logical and practical reasons to coordinate much of the management, authority, resources, and accountability for personnel security through military service-level organizations, and to use a parallel model for other DoD components and industry. For the military services, which are the primary users of the personnel security system, we believe that this coordination of administration and accountability at service-level organizations will help the services to better control a personnel process that impacts military operations. We argue that a new DoD office—DITTO—should be created to operate, budget for, and evaluate an integrated information technology architecture to serve the system-wide needs of the personnel security system, such as rapid and secure data exchange, functional evaluation, and data-based modeling and prediction. Thirdly, we suggest that the PSOC be framed as a committee to review proposed policy and funding changes, comprised of flag-level representatives from the components, and chaired by a C3I S&IO SES-level Director. The PSOC would be charged with responsibility for overseeing the DoD personnel security system and would include technical and other subcommittees as necessary.

In terms of expected improvements over the current personnel security program, the RAMPs/DITTO model should yield multiple benefits, such as:

- Increased ability for the military services, DoD agencies, and industry to predict personnel security requirements and to manage the process.
- Greater work efficiency through improved data and document transfers, file access, and integration of related databases.
- Improved management of information systems, technical support, and technology life-cycle planning.
- Improved ability to assess, report, and predict performance and resource utilization for individual organizations and the overall system.
- Improved system-wide operational oversight and program management.

Although the purpose of this report was not to lay out complete operational details, several examples of operational alternatives were presented. Overall, we show that the RAMPs/DITTO model offers flexibility and adaptability to peacetime operations and sudden military actions. It can accommodate currently emerging program initiatives as necessary. In essence, this report provides a blueprint of a future DoD personnel security system. Much work remains in applying this blueprint to create a better system. To this end we propose the following recommendation.

Recommendation

Because the DoD personnel security system affects all DoD components, we recommend that an "Acting Personnel Security Oversight Committee" (APSOC) comprised of representatives of DoD components be established to manage the process of reviewing and acting on changes suggested by this report. The APSOC should be chaired by an SES-level staff member of C3I/S&IO. Tasks for the APSOC should include:

1. Circulating the RAMPs/DITTO report for coordination and comment to appropriate managers at the Army, Navy, AF, DIA, NSA, JCS, WHS, and industry.
2. Developing a Statement of Work (SOW) to be used in soliciting proposals for one or two Independent Planning Studies (IPS) on creating DITTO (see details, below).
3. Securing funding for one or two IPSs on creating DITTO.
4. Overseeing the development of predictive models of personnel security requirements, including:
    a. tasking the Army and Navy to pursue the development of personnel security requirements models that capitalize on current achievements and knowledge gained through the Air Force model-building effort, and
    b. coordinating with efforts at DSS's Central Requirements Office (CRO), which has conducted a survey of defense contractors to explore requirements prediction methods for industry.
5. Finalizing and submitting the Draft DoD Strategic Plan for Personnel Security to the ASD C3I for authorization and promulgation.
6. Developing operational plans for each proposed RAMP, including:
    a. estimating billets needed,
    b. outlining budget considerations, and
    c. developing plans for interim RAMP functioning, i.e., transition plans for establishing each RAMP prior to the completion of DITTO.
7. Overseeing efforts to maximize coordination of current initiatives such as JPAS, Phasing, and ACES, and communicating with the Chief Information Officers Council regarding government-wide IT issues that apply.
8. Deciding on the pursuit of related RAMPs/DITTO R&D projects, such as:
    a. developing an Adjudication Decision Support System, and
    b. developing a computer simulation model of the personnel security system.

Details for Independent Planning Studies of DITTO

Because the role of DITTO is to link DoD Components and industry, RAMPs, and PSI providers together with integrative information technology that supports the current and foreseeable needs of the personnel security system, the development of DITTO will be critical to the functioning and success of the entire personnel security system. Due to the challenges of developing an integrative IT architecture, DITTO will also be complex and expensive. Consequently, we recommend that one or two IPSs be conducted to generate a detailed plan for the development of DITTO. Each IPS could be performed by a DoD Federally Funded Research and Development Center (FFRDC) or similar contractor. Although funding a single IPS may be sufficient and less costly, funding two IPSs would allow C3I to compare two independent visions of creating DITTO and then to choose either the stronger plan or a synthesis of strengths from the two plans. Each IPS is estimated to cost between $250K – and $450K.

The IPS effort(s) should be driven by a Statement of Work (SOW). Thus, one task of the APSOC is to oversee the production of a SOW for the IPS. The SOW should include a statement of objectives, a systems operation concept, and statement of requirements to drive the efforts of each IPS. The SOW should also require each IPS report to include information formatted to the needs of C3I POM submission documentation. At a minimum, the IPS SOW should stipulate that each IPS would produce:

1. a detailed architectural description (C4ISR[14] compliant),
2. cost and schedule estimates for full system development, including Costs As an Independent Variable[15],
3. a documented Analysis of Alternatives, including considerations for using parts or all of CCMS,
4. a transition plan for moving from current DoD systems to the proposed system, and
5. a recommended acquisition approach, including attention to Clinger-Cohen Act (1996) and MAISARC/MAISAP (DoD 5000.2R, 2001)[16] requirements.

This report outlines why a new model of the DoD personnel security system is necessary, several attributes of an ideal model, and a specific RAMPs/DITTO vision of how those attributes could be reified into an improved personnel security system. The report recommendation for establishing a managing committee is an acknowledgement that, although a specific vision is necessary for productive discourse and planning, success depends on effective execution. By managing the review and implementation of the tasks outlined above, we believe the APSOC can coordinate the interests of the DoD components, drive visionary and practical improvements throughout the DoD personnel security community, and strengthen the program's ability to serve DoD.

[14] Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) programs pertains to guidelines regarding how DoD collects, processes, produces, disseminates, and uses information.

[15] The Defense Acquisition Deskbook defines Costs As an Independent Variable (CAIV) as, "a strategy that entails setting aggressive, yet realistic cost objectives when acquiring defense systems and managing achievement of these objectives. Cost objectives must balance mission needs with projected out-year resources, taking into account existing technology, maturation of new technologies and anticipated process improvements in both DoD and industry."

[16] A Major Automated Information Systems Acquisition Review Council (MAISARC) reviews each Major Automated Information Systems Acquisition Program (MAISAP). These designations refer to AIS acquisition programs that are: [1] designated by the ASD(C3I) as a MAISAP, or [2] estimated to require program costs in any single year in excess of $30 million in FY 1996 constant dollars, total program costs in excess of $120 million in FY 1996 constant dollars, or total life-cycle costs in excess of $360 million in FY 1996 constant dollars.

References

Bosshardt, M.J. (2000). *Issues in developing a new conceptual framework for the DoD personnel security program* (Technical Report 361). Minneapolis, MN: Personnel Decisions Research Institute.

Chandler, C.J., & Timm, H.W. (2001, August). Automated Continuing Evaluation System (ACES): Project status and fast track implementation issues. Briefing to J. William Leonard, then Deputy Assistant Secretary of Defense (Security and Information Operations).

Clinger-Cohen Act of 1996, P.L. 104-106 (2000, November 30). *Management of federal information resources*. Office of Management and Budget Circular A-130.

Cox, Lt Col., (2001, February). DSS CCMS Information Systems Joint Program Management Review. Briefing to Lt Gen (Ret) Cunningham.

Defense Personnel Security Research Center. (2000). *DoD Strategic Plan for Personnel Security* (draft). Monterey, CA: Author.

Defense Security Service: How big is the backlog of personnel security investigations? (2000, September). Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform, 106th Cong., 2d Sess. Serial No. 106-267.

Defense Security Service: Mission degradation? (2001a, March). Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform, 107th Cong., 2d Sess. Serial No. 107-40. (testimony of Dennis Kucinich).

Defense Security Service: Mission degradation? (2001b, March). Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform, 107th Cong., 2d Sess. Serial No. 107-40. (testimony of Christopher Shays and Arthur L. Money).

Defense Security Service: Mission degradation? (2001c, March). Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform, 107th Cong., 2d Sess. Serial No. 107-40. (testimony of J. William Leonard).

Director of Strategic Plans and Policy (2000, June). *Joint Vision 2020*. Washington, DC: U.S. Government Printing Office.

DoD Inspector General (2001, February 28). *DoD adjudication of contractor security clearances granted by the Defense Security Service*. Washington, DC: Author.

DoD 5000.2-R (2001). Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs; 10 June 2001.

DoD Instruction 4630.8 (2001, July 30). Procedures for interoperability and supportability of information technology (IT) and national security systems (NSS), Section 4.1.

DoD Industrial Security Review Committee (1984, December 10). *Analysis of the effectiveness of the Department of Defense industrial security program and recommendations for program improvement* (“Harper” report), p. 24. Report to the Deputy Under Secretary of Defense for Policy. Washington, DC: Author. (FOUO).

Duval, E., Hodgins, W., Sutton, S., & Weibel, S.L. (2002). Metadata principles and practicalities. *D-Lib Magazine, V8*, #4.

Exec. Order No. 12968, *Access to Classified Information*, 32 C.F.R. Sec. 3.2(b) August 2, 1995; Security Policy Board, Uniform Adjudicative Guidelines, March 24, 1997. 32 C.F.R. Part 47, Subpart B.

Heuer, Jr., R.J., & Crawford, K.S. (2001). Decision options for implementing phased reinvestigations in DoD (MR-01-3). Monterey, CA: Personnel Security Research Center. (FOUO).

Joint Personnel Adjudication System (JPAS, 2001). Website: https://jpas.bolling.af.mil/

Joint Security Commission. (1994). *Redefining security: A report to the Secretary of Defense and the Director of Central Intelligence*. Washington, DC: Author.

Management Challenges Confronting the Defense Security Service. (2000, February). Subcommittee on National Security, Veterans Affairs, and International Relations of the House Committee on Government Reform, 106th Cong., 2d Sess. Serial No. 106. (testimony of Christopher Shays).

Marchiori, C. (2002, January). USAF Personnel Security Investigative Requirements Process. Briefing to Security and Information Operations (S&IO/C3I/OASD).

Marshall-Mies, J.C. (2001). *Survey of methods and plans for projecting personnel security investigations requirements.* Arnold, MD: Swan Research, Inc.

Office of Management and Budget. (1999). OMB Circular No. A-76, *Performance of Commercial Activities*.

Office of Management and Budget. (1996). Raines’ rules on federal information systems investments. Washington, DC: Author.

Paller, R. (2002, March). TAPSIMS Demonstration. Briefing by the Office of the Deputy Chief of Staff, G2 (Department of the Army).

Personnel Security Investigations Process Review Team. (2000a, October). *An assessment of the DoD personnel security program.* Report to the Deputy Secretary of Defense. Washington, DC: Author.

Personnel Security Investigations Process Review Team. (2000b, October). *An assessment of DoD's plan to eliminate the periodic reinvestigation (PR) backlog*. Report to the Deputy Secretary of Defense. Washington, DC: Author.

Personnel Security Managers' Research Program. (2002). Divided national loyalties: A primer for personnel security staff. Washington, DC: Author.

Projection of Personnel Security Requirements for Industry: A Survey. (2002). Defense Security Service, Industrial Security Directorate. Alexandria, VA.

Public Law 105-270, Oct. 19, 1998 *Federal Activities Inventory Reform Act of 1998.*

Rosenthal, A., Manola, F., & Renner, S. (2000). Getting data to applications: Why we fail, how we can do better. Bedford, MA: The Mitre Corporation.

Sands, W.A. (2001). *Development of a personnel security clearance adjudication decision support system for the Department of Defense: A feasibility study* (CRA Report 2001-01). San Diego, CA: Chesapeake Research Applications.

Sands, W.A. (2001). *Development of a computerized simulation model of the personnel security clearance process for the Department of Defense: A feasibility study* (CRA Report 2001-02). San Diego, CA: Chesapeake Research Applications.

Threats to U.S. national security: Statement for the Record before the Senate Select Committee on Intelligence, 104th Cong. (1998) (testimony of Louis J. Freeh).

TRW's In-Progress Review of DSS CCMS Remediation Activities, One Year Later: Final Report. (2000). TRW Inc., Systems and Information Technology Group.

U.S. General Accounting Office. (2002, April 5). *Electronic government:Challenges to effective adoption of extensible markup language.* (GAO-02-327). Washington, DC: Author.

U.S. General Accounting Office. (2001a, April 3). *Information and technology management: Achieving sustained and focused governmentwide leadership* (GAO-01-583T). Testimony before the Subcommittee on Technology and Procurement Policy, House Committee on Government Reform (statement by David L. McClure).

U.S. General Accounting Office. (2001b, April 18). *DOD personnel: More consistency needed in determining eligibility for Top Secret security clearances*, p. 41 (GAO-01-465). Washington, DC: Author.

U.S. General Accounting Office. (2001c, May 8). *DOD financial management: Integrated approach, accountability, and incentives are keys to effective reform*, p. 8 (GAO-01-681T). Washington, DC: Author.

U.S. Office of Management and Budget. (1992, September 23). Office of Federal Procurement Policy (OFPP) Policy Letter 92-1 to Heads of Executive Agencies and Departments. *Inherently Governmental Functions.*

U.S. Office of Personnel Management Investigations Service (1999, July). *Personnel investigations processing system*. Washington, DC: Author.

Yoemans, M. (2000, March). Advancing knowledge management in DoD. Presentation to the High Performance Computing Communications Conference.

Appendix A

Comparison of Personnel Security Programs at Selected Federal Agencies

Comparison of Personnel Security Programs at Selected Federal Agencies

The text and table in this appendix summarize the practices of five representative federal agencies that do background investigations and adjudications of security clearances: DoD's DSS, OPM, the Department of Energy (DOE), the Central Intelligence Agency (CIA), and the National Reconnaissance Office (NRO). Several important historical developments are also noted. Across these agencies key differences include the:

- volume of clearances that must be processed and how long processing takes,
- co-location or physical separation of functional specialties within the system, and the consequent ease of interaction between specialists,
- degree to which processing of clearances relies on information technology,
- degree of reliance on federal investigators as opposed to contractor investigators,
- degree to which "clean case screening" procedures are used.

The total volume of clearances varies greatly across agencies. In 2000, some 2.1 million DoD personnel held security clearances. DOE accounted for approximately 105,000 clearances, and roughly 80% of persons working at DOE facilities are contractors, not DOE employees. The size of the workforces at CIA and NRO remains classified. As discussed earlier in the main body of this report (see section "Comparison of Investigation and Adjudication Across Federal Agencies"), the volume of clearances processed per year affects what is operationally feasible.

The physical locations of the various personnel security specialists grew out of the circumstances of the organizations' founding and history, but these locations also express the relationships each agency assumes among the various functions. The most centralized structure among the agencies compared here is found at CIA, where a combination of in-house and contractor units do background investigations and in-house adjudicators make decisions based on those investigations.

In contrast, DOE exemplifies the most decentralized structure. DOE's personnel security program emerged from the need to ensure that only trustworthy employees handled restricted data or special nuclear materials at various sites across the country. A site-specific focus has persisted since the late 1940s. DOE invests 11 sites around the United States, some of which work with nuclear materials, with the responsibility for initiating and tracking security clearances for personnel at that site.[17] DOE has never been granted authority to conduct personnel investigations. Its background investigations are conducted either by OPM or, for certain high-risk positions, by the FBI. If in turn OPM or the FBI contracts for investigations, DOE does not have input into this decision. The DOE personnel security specialists at each site who compile records and track cases do a variety of tasks, and at small offices they may perform duties in addition to personnel security functions. Personnel security specialists at each location adjudicate clearances for personnel at that site (Gebrowsky, 2001).

[17] The 11 sites are: Richland, WA; Idaho Falls, ID; Oakland, CA; Las Vegas, NV; Albuquerque, NM; Chicago, IL; Pittsburgh Naval, PA; Schenectady Naval, NY; Savannah River, GA; Oak Ridge, TN; and Washington Headquarters in Germantown, MD.

DSS and OPM are larger and more multifaceted organizations than either CIA or DOE, and their structures reflect these demands. Both operate from headquarters in the greater Washington D.C. area that are supported by regional and district offices distributed nationwide. DSS has five regional headquarters and some 80 field offices; OPM's current investigative provider, USIS, has four regional offices, 48 district offices, and 180 Investigator Duty Station offices.

The intent of the consolidation of DoD's resources for background investigation of its personnel into DIS in 1972 was to increase efficiency and improve the quality and timeliness of investigations. The goal was to create a single professional cadre of government civil servants who would investigate all DoD personnel who needed access to sensitive information. In 1980 further consolidation brought under DIS the Defense Industrial Security Program and its organizational expression, the Defense Industrial Security Clearance Office (DISCO) along with the DoD Security Institute (DoDSI) to provide training. This consolidation concentrated the burgeoning security program for contractors and the training of security personnel at DIS. In 1992 DIS added counterintelligence to its capabilities, and in 1997 it assumed the name Defense Security Services.

DoD procedures deliberately keep the investigator and the adjudicator organizationally and physically separate. In earlier periods this goal was not so clear-cut. Before the consolidation that produced DIS in 1972, both investigation and adjudication functions were handled within the military components in various configurations, and since 1965 industrial clearances were tracked and adjudicated, but not investigated, by DISCO.

In 1984 DOD launched an investigation into industrial security practices in response to the serious espionage cases by contractor employees Christopher Boyce and James Durwood Harper. The report by the "Harper Committee," published in December 1984, raised the issue of potential unfairness to the applicant if the agency doing the investigation (in this instance DIS) also adjudicated the clearance. Since DISCO did all adjudications for contractors, and since DISCO became part of DIS in 1980, in effect the same organization was then performing both functions, albeit with different personnel.

The report cited the Administrative Procedure Act (5USC 554d2) and the Attorney General's manual on this act, which characterized the law as "intended to maintain the independence of hearing officers, and as a practical matter this means that an agency's hearing examiners should be placed in an organizational unit apart from those to which investigative and prosecuting personnel are assigned…" (DoD Industrial Security Review Committee, 1984, p. 24). There followed a discussion of whether this applied to personnel security adjudication hearings or not, since all personnel security actions take authority ultimately from the Executive Order, while the law specifically refers to programs created by statute. The Harper Committee study suggested that would be better for DoD to be safe rather than sorry and to keep them separate, reasoning that "If the program is not within the scope of 554 APA there may still be due process and functional concerns where an agency exercises both investigative and adjudicative functions." (DoD Industrial Security Review Committee, 1984, P. 25).

Following the Harper Committee's recommendations, DoD undertook several reforms in the mid-1980s that widened the separation between the investigation and adjudication functions based on the belief that the law required it and that it seemed desirable. For example, in June 1985, DISCO's Adjudication Division was transferred out of DIS and into a division in the DoD Office of General Counsel. This move created the desired organizational separation for adjudicators from DIS as the investigative agency. However, screening procedures for contractor employees on-going at DIS (now DSS) since 1984 still raised questions about whether the same agency doing investigations is also in effect doing adjudications, as noted in a DoD Inspector General audit of February 2001 (DoD Inspector General, 2001). Thus the supposed necessity to keep these functions separate and issues about how to disentangle them remain lively concerns in DoD.

Ostensibly both OPM and NRO handle background investigations similarly in that they use contractor investigators. Currently, USIS is OPM's sole investigation provider, however due to the heavy workload OPM is in the process of obtaining a supplemental provider. USIS regularly competes against other providers for business. Although USIS has operated as a private company for six years, many of its field agents came with previous experience as federal investigators for OPM and other investigative agencies such as the FBI. USIS, on behalf of OPM conducts background investigations for approximately 100 federal agencies. DoD's personnel security investigations are only one of those 100 federal agency customers. USIS submits DoD background investigations to OPM, which forwards them for adjudication to one of DoD's eight CAFs.

The National Reconnaissance Office (NRO) is a hybrid agency that straddles DoD and CIA in its mission to manage the development and operation of intelligence satellites. Its funding and its personnel come from both DoD and CIA; staff members usually serve a tour of duty at NRO and then return to their sponsoring agency. Contractor employees are closely integrated with government staff at NRO due to the oversight the agency maintains over contractor companies supplying space technologies. NRO's approach to personnel security is also eclectic. All background investigations for NRO are contracted out, and since persons seconded to NRO from other agencies were usually issued access eligibility there, most of NRO's access determinations are for contractor employees. In-house adjudicators make decisions on access eligibility for NRO, and limited interaction between investigators and adjudicators occurs during the investigative process. NRO grants a "conditional clearance" in some cases in which issues arise, and then monitors the employee to ensure that conditions are being met. Through various mechanisms monitoring is a direction other agencies are taking as well. For example, the Washington Headquarters Service (a DoD CAF) may issue a warning letter in which a subject is told that although adjudication has granted the person a clearance, the investigation has noted questionable behavior, and that if the behavior continues, the clearance will be revoked.

Some agencies have evolved personnel security procedures tailored to their special needs. DOE, for example, offers an "Accelerated Access Authorization Program" (AAAP) that grew out of a situation in which particular personnel were needed quickly to respond to a rare clean up of materials. The program proved useful as a method for ensuring that interim clearances for some sensitive positions are granted on the basis of additional information. It consists of a specified set of evaluations done at either Albuquerque, NM or Oak Ridge, TN: a CI-scope polygraph, a drug screen, a psychological evaluation, an interview, a completed SF86 filled out at the site, and results received from an National Agency Check (NAC) into criminal history. The DOE Director of Security then grants an interim clearance, and the case is simultaneously sent for the typical background investigation followed by adjudication, since accelerated access is only an interim clearance. This AAAP clearance takes DOE about 17 to 27 days to complete, including two full days for the applicant on site plus waiting for the NAC, drug screen, and polygraph results. DOE processed roughly 150 of these AAAP clearances in 2000.

Both CIA and NSA have evolved accelerated or concentrated screening procedures that are tailored to the needs of each of those agencies. DoD CAFs also issue interim clearances (while an investigation is on-going) based on favorable checks of national agency databases. These interims are issued in a matter of days for lower level clearances and in 30 to 45 days for an interim Top Secret clearance.

Table A.1 (below) summarizes key differences among the five agencies under discussion: DSS, OPM, DOE, CIA, and NRO. The resulting suggestions we derive from this comparison for improving the DoD personnel security program appear earlier in this report (see section, “Comparison of Investigation and Adjudication Across Federal Agencies”).

Table A.1
Comparison of Federal Personnel Security Programs

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
Composition of PSI personnel: what are the people called who are on the team?	• Personnel Security Assistant (PSA) • Case Analyst (CA) • Special Agent (SA) • CAF adjudicator	• Data Transcriber • Reviewer • Adjudicator • Investigative Inquiry Specialist • Special Investigator • Record Searcher / Record Specialist / Record Courier	• Personnel Security Specialist (PSS)	• Investigator (several branches) • Records Manager • Case Manager (who serves as the adjudicator) • Personnel security administrators. • Personnel security experts.	• Customer Relations Specialists • Investigative Management Systems personnel • Contract Field Investigators • Special Actions Staff • Special Investigations.
Locations of the PSI personnel: where is everybody?	• DSS personnel are at DSS HQ in Alexandria, VA, and in Linthicum, MD; at the PIC in Ft. Meade, MD; at DISCO in Columbus, OH; or at DSS field throughout the United States and in Puerto Rico. • Contractor investigation companies located in DC area, with field offices elsewhere • CAF adjudicators are at 8 CAFS in the Washington D.C. area and in Columbus, OH.	• OPM-FIPC personnel are in HQ office in Boyers, PA • USIS, a "sole-source contractor," consisted in 1996 of 400 federal Investigators who turned into a private company. HQs in Annandale, PA, with 4 regional offices, 48 district offices, and 180 investigator duty	• At 11 offices around the country, personnel security specialists initiate, adjudicate, and track clearances at the sites for which they are responsible. • DOE personnel security investigations are performed by either OPM or the FBI .	• All personnel security staff are domestically located.	• Adjudicators are located at the NRO Personnel Security Division along with the Investigative Management Systems personnel who initiate and track cases • All investigations are contracted out • NRO staff members come from other

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
		station offices			agencies. NRO straddles DoD and CIA, with staff from both.
Extent of interaction between investigators and adjudicators: who talks to whom?	• No interaction is structured between the adjudicator and the case analyst, or the adjudicator and the special agent.	• The contract company USIS does personnel security investigations, and no interaction with DoD adjudicators is structured.	• There are no DOE investigators because DOE does not hold authority to conduct personnel investigations. • Personnel security specialists adjudicate cases..	• When feasible, interaction between investigators and adjudicators is facilitated.	• The contract company does investigations, and no interaction with adjudicators is structured.
Timeliness for completing PSIs: how long does it now take, for example, to get a TS clearance?	• 330 days [2000]	• OPM has four service type categories; 35/75/120/180 days. The timeliness service requested by the customer dictates the applicable completion time category.	• Q clearances: 60 days at Albuquerque, • 90 days on average across the 11 sites	• No information	• No information.
Number of Clearances Currently held	• FY2000: roughly 2.1 million total in DoD • Confidential: 74,795 • Secret: 1,571,780 • Top Secret: 211,566 • TS-SCI: 263,599	• DoD figures, see DSS	• 105,000 in DOE, 70,000 Q 35,000 L	• [classified]	• [classified]

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
	• Total: 2,121,740*				
Use of capabilities of information technology: how are computers, automated decision systems, etc. used?	• CCMS used for tracking cases, as the database of info from investigations, and for report generation • CCMS does autoscoping, but the CA also reviews this to add or delete leads ased on prior files, and to reflect special project demands. • Field investigators print out paper "Action Lead Sheets (ALSs)" from the electronic file sent in the "Field Investigation Management System," which converts CCMS data into leads. Use of ALSs facilitates data entry while doing personal interviews	• Case tracking in PIPS allows requestor to query status on-line • Automated decision logic in PIPS opens case, does scoping, generates automated data requests to other agencies, generates scannable investigation forms, and generates reports • Field investigators use laptops to generate and submit electronic ROIs	• Each of the 11 sites enters cases into a regional database using an IT system, and this information feeds into a central adjudicative database.	• Automated case tracking. • No information on system specifics.	• In-house NRO database and tracking of cases • No information on the specifics of what system they use or details of its use.
"Clean case screening": is it done, and in what circumstances?	• Yes: for industry cases only, DSS CAs at the PIC uses a screening guide to identify "clean cases" which are entered into CCMS, archived, and sent to DISCO for a second review, then for issuance of clearance, unless an issue is found that	• No information on clean case screening.	• The personnel security specialist reviews the investigation report and screens it for derogatory information. Cases with no derogatory information are adjudicated. The	• No information on clean case screening	• No information on clean case screening. • NRO grants "conditional clearances" with a monitoring program to ascertain whether conditions are being met

Options-relevant Issues	DSS	OPM/USIS	DOE	CIA	NRO
	demands adjudication by DOHA. •		personnel security specialist follows up cases with derogatory information. After adjudication has been made, an appeals procedure is available. Appeals go to the Director of Security.		
Extent of reliance on in-house vs. contractor investigators	• DSS uses both in-house and contractor investigators. • DSS has approx 1400 in-house field investigation agents, and 1900 total in-house employees • DSS also uses six contractors providing PSIs in FY01: Dyncorps, Mantech, GBSG, MSM, OPM/USIS, Omniplex •	• OPM relies entirely on contractor investigators, and USIS is the sole source • 2,067 employee field investigators and 507 contractor investigators work for USIS, performing all Special Investigator functions.	• DOE does not hold authority to conduct personnel investigations. By law its investigations are performed by OPM or, for certain high-risk positions, by the FBI.	• Not available.	• NRO relies on contractor investigators.
Distinctive aspects	• DSS, as an agency of the federal government, is one expression of the government's "stake" in personnel security; the CAFS are a	• OPM advances completed investigative case material to customers "closed pending" when certain	• DOE's approach to personnel security was shaped in part by its history as an agency that controls nuclear	• Much smaller than DSS's universe in DoD or USIS's universe in OPM. Has a	• NRO is much smaller than DSS's universe in DoD or USIS's universe in OPM, and NRO has a

Options-relevant Issues	**DSS**	**OPM/USIS**	**DOE**	**CIA**	**NRO**
	second.	source information is still pending. This allows the customer to make risk management decisions based upon the bulk of the timely, completed investigative material • PSIs are only one fraction of OPM's personnel investigations for many federal agencies, and security is only one of OPM's personnel functions for the federal government.	materials at various locations. A decentralized system of 11 regional offices has evolved. • DOE uses an Accelerated Access Authorization Program that allows interim clearances to be granted more quickly while a regular investigation and adjudication is ongoing.	specialized intelligence-related mission. • The hiring process includes a thorough medical examination of one's physical and mental fitness to perform essential job functions.	specialized space R&D mission. • Almost all of their personnel come from other federal agencies. • 80% of all clearances granted at NRO are for contractors. • NRO is an example of a DoD agency that contracts directly with a PSI provider.

Appendix B

Excerpts from the Final Report on Survey of Methods and Plans for Projecting Personnel Security Investigations Requirements

Excerpts from the Final Report on: *Survey of Methods and Plans for Projecting Personnel Security Investigations Requirements*

Requirement

This effort supports research regarding *Options for Future Defense Personnel Security Systems* (the "Options" project), initiated by the Deputy Assistant Secretary of Defense for Security and Information Operations, Command, Control, Communications, and Intelligence (DASD(S&IO/C3I)). The goal of the Options project is to strengthen the DoD personnel security program's ability to manage the challenges of the coming decade and beyond. The current effort supports an Options project focus on understanding the derivation and improving the prediction of personnel security requirements by: (1) exploring quantitative and qualitative methods currently being used by military, civilian government, and industrial organization leaders to estimate Personnel Security Investigations requirements for one to five years in the future; (2) obtaining feedback on a "straight-line" method of projecting requirements; and (3) seeking recommendations to improve the derivation and projections of personnel security requirements.

Methodology

Ten industries, three military services, and two government agencies were selected to participate in this effort because their projected PSI requirements were among the highest within the DoD for the year 2002 through 2007. Projections for these organizations included initial investigations and PRs for positions requiring access to Sensitive Compartmented, Top Secret , Secret, and Confidential Information and for positions designated as Positions of Trust. Also, in the case of the military services, these projections included requirements for Entrance National Agency Checks (ENTNACs) for military accessions and NAC(T)s for Positions of Trust.

Respondents who participated in a telephone interview were individuals responsible for providing DSS with their organization's projected PSI requirements for the years 2002 through 2007. These respondents were asked to provide insights and suggestions concerning how their organization generated these estimates and what data and methods might be available to improve future estimates.

For the sake of clarity and brevity, the following reference codes are used to refer to the number and types of organizations that responded in a certain way:

- IND refers to industrial contractors;
- MIL refers to military services; and
- GA refers to government agencies.

For example, the code "8/10 IND" indicates that the findings pertain to 8 of the 10 industries surveyed; the code 1/3 MIL indicates the findings pertain to one of the three military services surveyed; and 1/2 GA indicates the findings pertain to one of the two government agencies surveyed.

Findings

Current Projection Methods

The respondents were first asked to describe their organization's current projection method and how closely this method resembled a "straight-line" method of projecting requirements. In these discussions, "straight-line" was defined as examining an organization's actual requirements over the last three to five years and projecting future years based on the observed trend, assuming that future requirements would follow directly from prior year requirements.

In general, each respondent described a slightly different approach to projecting PSI requirements. None of the respondents reported using a pure "straight-line" method. However, four respondents (2/10 IND, 2/3 MIL, 0/2 GA) described a "modified straight-line" approach, wherein they started with "straight-line" projections and then adjusted these projections to take into account other variables, such as changing accession rates, retirements, and new policies. The remaining respondents (8/10 IND, 1/3 MIL, 2/2 GA) reported that they combined several different types of current and estimated data to derive their projections. Apparently, these respondents employed expert judgment to combine disparate data elements into projections of future requirements. The projection process was summarized n the words of one respondent who said, "Projections are not a science."

In the sections below we describe the major elements that respondents reported taking into account in projecting PSI requirements.

Cleared Populations and Projected Requirements

The military services provided PSI requirements projections for military and civilian government positions requiring access to SCI, TS, S, and C information, as well as entrance requirements for military personnel and Positions of Trust. The government agencies provided projections for civilian government positions and for upgrades to military positions requiring access to SCI and TS information. Industry provided contractor requirements estimates for positions requiring access to SCI, TS, S, and C information and for those designated as Positions of Trust.

Organizational requirements for initial and PR investigations varied considerably depending on the level of access required by the positions. For example, personnel in all civilian and military positions within the two government agencies that participated in the study required access to SCI or TS information. In the military services, access is a function of one's assignment; this was complicated by the fact that cleared personnel regularly move between assignments in cleared and non-cleared positions. Typically, all officers require clearances as do enlisted personnel in cleared Military Occupational Specialties (MOSs) or ratings. Civilians in cleared positions also require clearances. Since cleared individuals only require access when assigned to certain positions, requirements for PR investigations were often difficult to predict.

Initial Investigations

Most of the respondents described their current projection methods for initial investigations as taking into consideration hiring and accession patterns, retirements and other attrition patterns, and anticipated growth. In addition, three-fifths reported that they incorporated specific program requirements and almost one-half reported that they used prior years' data as a baseline for their PSI projections.

- ***Hiring and accessions patterns.*** Respondents in most of the organizations took hiring and accession patterns into consideration in their initial investigations projections. (10/10 IND, 2/3 MIL, 1/2 GA)

- ***Retirement and attrition patterns.*** Most respondents also included information on retirements and other attrition patterns in their projections (10/10 IND, 1/3 MIL, 1/2 AG).

- ***Anticipated growth rates.*** Anticipated growth rates were factored into most organization's projections (10/10 IND, 1/3 MIL, 2/2 GA). Such growth was based on strategic plans, proposals in the pipeline, and/or upcoming additions to current contracts. However, several respondents stressed that they conducted a "sanity check" in order to correct the overly optimistic projections provided by those responsible for new business (2/10 IND, 2/3 MIL, 0/2 GA).

- ***Specific Program Requirements.*** Data on specific program requirements were gathered from program managers and input into projections by Security personnel in three-fifths of the organizations (6/10 IND, 2/3 MIL, 1/2 GA). As with new business projections, several respondents mentioned the need for "sanity checks" of projections provided by program managers (2/10 IND, 2/3 MIL, 0/2 GA).

- ***Baseline data.*** For purposes of this study, the term "baseline" referred to data concerning actual investigations that had been requested, opened, and/or closed during the previous year or two. Approximately half of the respondents indicated that they used such baseline data in their projection model. (4/10 IND, 1/3 MIL, 2/2 GA)

Periodic Review Investigations

Most organizations reported using methods such as querying databases of cleared personnel, reviewing historical data, top-down extrapolations, and field data calls to develop requirements estimates for PRs. Instead of these more direct methods, several organizations simply applied a formula to their cleared population to estimate the PRs for future years.

- ***Database queries.*** Approximately three-fourths of the respondents described a process whereby they queried their cleared personnel database to project PRs based on employees' initial or last investigation dates. For example, those cleared at the SCI or TS level, who had an initial or last investigation date of 2001, would likely require a PR in 2006. This method assumed a relatively stable workforce in which cleared personnel who leave the workforce would be replaced on a regular basis. (9/10 IND, 1/3 MIL, 1/2 GA)

- ***Review of historical data.*** Approximately half of the organizations reported using historical data to inform PR projections. These organizations reviewed PSI requirements projected and fulfilled over the last several years and used these historical patterns to project future requirements. (5/10 IND, 3/3 MIL, 0/2 GA)

- ***Top-down extrapolations.*** Since data required to make accurate projections were not readily available or as accurate as desired, one respondent employed a top-down approach in which PSI requirements were extrapolated from strategic plans and policies. This respondent reported that the organization had recently undertaken efforts to improve the quality of the projection data it receives from its commands and subcommands. (0/10 IND, 1/3 MIL, 0/2 GA)

- ***Field data collection.*** Two respondents described their organizational structures as decentralized. In these organizations local commands or subcommands maintained their own security-related access data. Therefore, Security personnel issued full or partial data calls to their field commands and subcommands to gather input to their PR projections. (0/10 IND, 2/2 MIL, 0/2 GA)

- ***Application of a PR formula.*** Only two respondents reported that they applied a formula to their total cleared personnel population to identify those who would need PRs over the next five years. This formula was based on an assumption that one-fifth of the cleared population would need PRs in each of the next five years. (1/10 IND, 0/3 MIL, 1/2 GA)

Databases and Other Resources

The two primary resources used by surveyed organizations to project PSI requirements were databases of cleared personnel and input from program managers.

Databases of Cleared Personnel. The quality of databases available to Security personnel for projecting PSI requirements varied considerably from organization to organization. Some databases were centralized across the organization; others were local, "homegrown" systems. Several respondents (2/10 IND, 2/3 MIL, 0/2 GA) reported that they had access to a centralized, organization- or corporate-wide database of cleared personnel. These centralized databases, which contained up-to-date personnel security clearance information, tracked actions such as ENTNACs, initial and last investigation dates, and position access codes. Although all respondents had access to the Meade Validation Listing, which is a centralized database of cleared DoD personnel maintained by DISCO, only one respondent mentioned using this information for developing projections (1/10 IND, 0/3 MIL, 0/2 GA).

The majority of respondents reported having access to local databases of cleared personnel containing initial and last PR investigation dates (9/10 IND, 0/3 MIL, 2/2 GA). Of particular note were two industries that had incorporated or linked personnel data such as personnel actions, reassignments, and attrition, into their clearance database. In addition, two industry respondents reported that they maintained separate Special Access Program (SAP) databases, and two reported having systems that tracked clearance requests from program managers. In all of these local and centralized databases, special queries could be designed to identify those who would need PRs within the next five years.

Program Managers. Almost half of the respondents reported that they incorporated input from program managers into their projections (5/10 IND, 1/3 MIL, 1/2 GA). In fact, two of these respondents from industry noted that program managers' input was regularly sent to, or coordinated with, Security personnel.

The respondents differed concerning the value or feasibility of using data from program managers in PSI projections. Supporters of the practice noted that program managers have the most accurate and up-to-date information about their programs and were regularly involved in projecting program requirements for internal organization use (1/10 IND, 1/3 MIL, 0/2 GA). Detractors commented that program manager's input did not improve projections (4/10 IND, 0/3 MIL, 2/2 GA). Specifically, they noted that program managers often were too optimistic, provided poor quality data, and inadvertently double-counted personnel who worked on multiple programs or moved among programs. In addition, three respondents expressed concerns about the feasibility of gathering such data due to the large number of program managers and the shortage of Security personnel within their organization (3/10 IND, 0/3 MIL, 0/2 GA).

Limitations to Current Projections

The respondents described a number of limitations to their current projections. These limitations varied considerably by type of organization.

Limitations on Projections by Military Service and Government Agencies. Respondents from the Military services and government agencies were particularly concerned with challenges they faced in dealing with contractor projections and uncertainties inherent in patterns of future hiring of contractors.

Challenges to projecting contractor requirements. Less than half of the respondents (3/10 IND, 2/3 MIL, 2/2 GA) noted difficulties in projecting contractor requirements. These difficulties were mainly due to inadequate contractor databases, which were described as "invalid," "of poor quality," or "non-existent." In a tedious attempt to develop a valid database of cleared contractor personnel, one government agency was verifying their clearance database by querying the DCII one person at a time to identify contractors who worked on agency contracts.

Other difficulties cited by two respondents (1/10 IND, 0/3 MIL, 1/2 GA) included the fact that their customers dictated the types of investigations needed for programs and their organization had a historical practice of making programs responsible for contractor requirements. Both practices kept Security personnel "out of the loop" so they were not in a position to adequately project program or new project PSI requirements. In order to address these problems, these two organizations recently created centralized databases of contractor requirements under the Security Office.

Uncertain future hiring patterns. Approximately half of the respondents (4/10 IND, 2/3 MIL, 1/2 GA) noted that their accession and retention patterns varied considerably from year to year. They noted that often their personnel assignment criteria did not match security requirements so they had no way of knowing which positions could be filled with already-cleared individuals and which will require new investigations or PRs. These respondents also anticipated increased use of contractors which would shift hiring patterns and would lead to more overlap in contractor projections made by both government and industry.

Limitations of Industry Projections. A majority of industry respondents emphasized limitations based on unpredictable business fluctuations and the volatility of contract assignments. A smaller number of industry respondents were concerned about the lack of validity of long-term predictions.

Unpredictable business fluctuations. All industry respondents and one military service respondent (10/10 IND, 1/3 MIL, 0/2 GA) emphasized that unpredictable business fluctuations limited their projections. The greater these fluctuations, the less accurate were the projections, especially since Security personnel were often not included in planning for contracts and new business.

Fluctuations included unforeseen corporate mergers or acquisitions and the unpredictable rate of success in winning contracts. If an organization were to win a large contract, such as the Joint Strike Force (JSF), its projections would increase dramatically. If it were to lose the JSF bid, it could possibly join the winning bidder as a subcontractor and still increase its cleared workforce, or it could lose cleared employees to the winning bidder.

Respondents mentioned other factors that affected industry's business flow. For example, economic changes and political developments had a direct impact on DoD funding and, in turn, on the number and size of government contracts. As these factors changed, industries adjusted their strategic plans, sometimes shifting back and forth between the "Black" (covert) and "White" contracting worlds or between national defense and commercial or international business. These factors had a direct impact on their volume of classified work and the stability of their workforce and, thus, their PSI requirements.

Volatility of contract assignments. Another factor mentioned by approximately half of the respondents (6/10 IND, 1/3 MIL, 1/2 GA) was the movement of cleared personnel from project to project both within and across industries. In addition, many contractor personnel worked on multiple projects within a company. These movements and work patterns were difficult to track, and often resulted in double and sometime triple counting of cleared contractor personnel, especially by program managers.

Invalid long-term projections. Several industry respondents (3/10 IND, 0/3 MIL, 0/2 GA) indicated that they considered projections beyond two years to be invalid, noting that their industry strategic plans were updated annually, oftentimes completely changing for the "out years." They were very uncomfortable projecting requirements beyond two or, at the most, three years.

Other Limitations

Respondents mentioned several other important limitations, including a lack of infrastructure to track/project requirements, unclear guidance for projection requests, varying procedures for requesting investigations, and difficulties predicting PRs.

Lack of infrastructure to track or project requirements. While most organizations had databases of cleared personnel, these systems were not originally designed to track and project requirements or to track investigations as they were completed (1/10 IND, 1/3 MIL, 1/2 GA). Only a few of these systems were centralized across the organization; most were local systems that included minimal data such as the date of the initial and latest investigation.

One respondent noted that, for purposes of projections, organizations had to make assumptions concerning the number of pending investigations that would be completed each month (1/10 IND, 0/3 MIL, 0/2 GA). Other individual respondents noted that there were often different criteria and operating procedures for requesting investigations within a given organization, data from the field included double counts of requirements, and field personnel were not trained to provide input to projections.

Unclear guidance and changing policies. A few respondents cited limitations due to unclear requests for projections and insufficient guidance for changing policy. One respondent noted that the DASD(S&IO/C3I)'s requests for projections were unclear and appeared to focus more on the numbers than on the quality or validity of the numbers.

Three respondents (1/10 IND, 1/3 MIL, 1/2 GA) indicated that the guidance for changing policy was also unclear. For example, recent policy required that personnel in information technology positions have background investigations even though they did not have access to classified systems or information. This policy change covered current as well as future contracts and increased the complexity and variability of the projection process.

Varied methods for projecting requirements. Lack of clarity in requests for projections and policy resulted in organizations using various methods to project requirements (1/10 MIL, 1/3 MIL, 1/2 GA). These different methods for gathering and summarizing projection data made it difficult to compare requirements across organizations and to assess the validity of these projections.

Difficulties predicting PRs. Five respondents indicated that their projections were affected by the large numbers of investigations pending or not completed as well as the changing PR submission requirements (5/10 IND, 2/3 MIL, 0/2 GA). One of these respondents noted that PRs did not always follow the anticipated pattern; sometimes employees left their position before the PR was due or a newly hired, previously cleared employee could need a PR immediately (1/10 IND, 0/3 MIL, 0/2 GA).

Another respondent stressed difficulties in projecting when personnel would need security access and, thus, need a PR (0/10 IND, 1/3 MIL, 0/2 GA). This was especially problematic for the military services since security access information was controlled and maintained at the local level.

Projection Rules of Thumb

The respondents were asked if they had developed any "rules of thumb" for projecting PSI requirements. Since these rules of thumb were often derived from historical data, they were typically unique to each organization. Also, the rules of thumb differed for initial and PR investigations.

Initial Investigation Projection Rules of Thumb

Examples of rules of thumb used by one or more organizations for predicting initial investigations follow:

- 40% of accessions require initial investigations. (0/10 IND, 1/3 MIL, 0/2 GA)

- Three SSBIs have to be requested for every SCI-level position that needs to be filled. This rule of thumb was developed because the organization was losing two of every three candidates while awaiting the results of the investigations. (0/10 IND, 0/3 MIL, 1/2 GA)

- A single industry respondent (1/10 IND, 0/3 MIL, 0/2 GA) mentioned each of the following rules of thumb for projecting initial investigations:

  - 10% increase in PSI requirements due to attrition and terminations

  - 25% attrition or turnover of new hires

  - 8% growth rate in PSI requirements based on the current five-year business plan

  - 17% turnover and a small number of retirements in SCI, TS, and Secret initial clearances, with a constant replacement by new hires

- 10% growth, assuming that most new hires already have clearances

  - One-third of all positions require a low level clearance to conduct work in international sales related to government work

PR Investigation Projection Rules of Thumb

Examples of rules of thumb used by one or more organizations for predicting PRs follow:

- One-fifth of all personnel cleared at the TS or higher level will need PRs during each of the next five years. (1/10 IND, 0/3 MIL, 1/2 GA)

- Projections, basing PRs on the last date of investigation, are reasonable since positions requiring access will remain filled even if current employees leave. (1/10 IND, 0/3 MIL, 0/2 GA)

- A single military respondent (0/10 IND, 1/3 MIL, 0/2 GA) mentioned developing the following rules of thumb for projecting PRs:
  - 60% of newly cleared personnel will require PRs within the five-year cycle. This rule takes into account naturally occurring attrition.
  - 60% to 70% of accessions, ages 16 to 18, will attrite before requiring a PR.
  - Losses at the Secret PR level will be 15% for accessions and 6% for Foreign Nationals.

Respondents' Recommendations for Improving PSI Requirements Projections

The final interview question asked respondents to recommend how PSI requirements could be improved. Among their recommendations were the following: change DSS policies and procedures, develop a generic DoD projection model, change investigation policies and procedures, improve PSI requirements data collection methods, clarify the role of the DASD(S&IO/C3I), and increase the budget and resources for projections.

Change DSS Policies and Procedures

Two-thirds of respondents recommended changes to DSS policies and procedures. Most frequently recommended was that DSS shorten its timeframe for projections (5/10 IND, 0/3 MIL, 0/2 GA), i.e., that projections for initial investigations be provided annually for a maximum of two years into the future. Respondents believed that their short-term projections were much more accurate than their longer-term, five-year projections. They had fewer objections to five-year PR projections since these projections were most often derived from current databases of cleared personnel. Only one respondent recommended a longer time frame in order to even out short-term fluctuations in requirements for initial investigations (1/10 IND, 0/3 MIL, 0/2 GA).

Other changes to DSS policies and procedures recommended by one or two respondents, were that DSS should:

- Establish and maintain a historical database similar to the one maintained by OPM. Once this database is established, DSS would be in a better position to create its own requirements projections. (0/10 IND, 1/3 MIL, 0/2 GA)
- Create ways to "flex" as demands change since there is no way to project requirements "on the money." Contracting out investigations based on the caseload was seen as one way to provide such flexibility. (1/10 IND, 1/3 MIL, 0/2 GA)
- Employ a service business model similar to civilian service organizations that work on a demand basis, e.g., Federal Express. In the words of one respondent, "Big business always operates from projections. Why can't DSS and the government do the same?" (1/10 IND, 1/3 MIL, 0/2 GA)

One respondent noted that, although DSS uses a fee-for-service business model, it still functions like an appropriated organization. This respondent recommended that DSS drop its fee-for service model for investigations and adjudications, noting that currently there is no way to validate charges, especially when contractors and cleared personnel work on multiple contracts and/or for multiple customers. (0/10 IND, 1/3 MIL, 0/2 GA)

- Review, standardize, and document in writing all DSS policies and procedures. This would result in a more consistent application of the investigation standards across investigators and localities and would help ensure comparable investigative products from all sources. (1/10 IND, 0/3 MIL, 0/2 GA)

Develop a Projection Model

Slightly over one-third of respondents recommended that the DASD(S&IO/C3I) develop a valid model for projecting investigative requirements (5/10 IND, 1/3 MIL, 0/2 GA). One to three respondents made the following additional recommendations:

- Since DISCO has a centralized PR database, it should project PR requirements. In one respondent's words, "It's ironic that you are talking to industry about PRs. DISCO has a database and knows when PRs are due. Why are you asking industry?" (3/10 IND, 0/3 MIL, 0/2 GA)

- Contractors should project requirements separately by contract. (1/10 IND, 0/3 MIL, 0/2 GA)

- DoD should create a joint government/industry team to address projection issues and to develop a uniform approach for all government and industry organizations to project PSI requirements (0/10 IND, 1/3 MIL, 1/2 GA). This team should:

    - Coordinate with the Aerospace Industry Association (AIA) which has been tracking issues related to DSS investigations for several years. (1/10 IND, 0/3 MIL, 0/2 GA)

    - Examine trend data relating the overall defense budget to PSI requirements. Such an analysis could provide "clues" to projections. (1/10 IND, 0/3 MIL, 0/2 GA)

    - Compare projected numbers with actuals as input to a mathematical model for projecting requirements. (1/10 IND, 0/3 MIL, 0/2 GA)

    - Develop a uniform approach for all organizations to project PSI requirements. This approach should allow for specific input to key variables, e.g., attrition or retirement rates. (2/10 IND, 1/3 MIL, 0/2 GA)

Change Investigations Policies/Procedures

Slightly over one-third of the respondents recommended changes to investigations policies and procedures (3/10 IND, 2/3 MIL, 1/2 GA). These recommendations, each from one or two respondents, included the following:

- Require that PRs be initiated at the end of four and one-half instead of five years. (1/10 IND, 0/3 MIL, 0/2 GA)

- Allow industry to set their own priorities as to the types of clearances that have most value to that industry. (1/10 IND, 0/3 MIL, 0/2 GA)

- Reduce clearance levels to two: one level for SCI and TS, and one for other levels, including positions of trust. This would result in fewer forms and types of investigations. (0/10 IND, 0/3 MIL, 1/2 GA)

- Reduce superfluous investigations by regularly updating PRs of MOSs or ratings that require SCI access even when individuals are not in positions that require access. (0/10 IND, 1/3 MIL, 0/2 GA)

- Develop a mechanism whereby all cleared military would be required to have an up-to-date PR in order to remain in a position that requires access. This would mean that individuals could not avoid PRs by moving between commands or assignments. (0/10 IND, 1/3 MIL, 0/2 GA)

- Develop a policy for waivers to clear a small number of consultants for a given project without requiring that the facility where the consultants work be cleared. (1/10 IND, 1/3 MIL, 0/2 GA)

Improve PSI Requirements Data Collection

Three-fifths of the respondents recommended improvements in the collection of PSI requirements data (5/10 IND, 2/3 MIL, 2/2 GA). These recommendations, each made by one or two respondents, included the following:

- The DASD(S&IO/C3I) should slow down its demand for projections until adequate tools are available. (0/10 IND, 1/3 MIL, 0/2 GA)

- The DASD(S&IO/C3I) should not assume that projections are the cure-all for the problems with the personnel security process. Many factors affect delays in, and the quality of, investigations. (1/10 IND, 1/3 MIL, 0/2 GA)

- Industry, not government, should identify contractor requirements. (0/10 IND, 0/3 MIL, 2/2 GA)

- For major programs, Program Managers should identify PSI requirements during the pre-development stages or start of a contract. (2/10 IND, 0/3 MIL, 0/2 GA)

- Government Program Managers should be required to predict requirements for their programs. (1/10 IND, 0/3 MIL, 0/2 GA)

- Require industry to maintain an up-to-date database of cleared personnel. (1/10 IND, 1/3 MIL, 0/2 GA)

- Decentralized organizations, such as the military services, should train Security Managers in the field to track and handle security requirements. They should also train enlisted personnel to support these Security Managers in maintaining databases and responding to requests for PSI requirements data. (0/10 IND, 1/3 MIL, 0/2 GA)

- Government and industry should develop ways to integrate data from Security as well as the Personnel System into their projections. (0/10 IND, 1/3 MIL, 0/2 GA)

Clarify the Role of the DASD(S&IO/C3I)

Several respondents recommended that the DASD(S&IO/C3I) clarify its role related to implementation of investigations and oversight of the projection process (1/10 IND, 2/3 MIL, 1/2 GA). Among these were recommendations that the DASD(S&IO/C3I):

- Take more responsibility for oversight in making and enforcing policies related to investigations. For example, it should ensure that the investigative standards and products are comparable across OPM, DSS, subcontractors, and other providers. (0/10 IND, 1/3 MIL, 0/2 GA)

- Provide clearer guidance to government and industry for developing projections of investigation requirements. For example, the DASD(S&IO/C3I) should clarify if and how interim clearances and Automated Data Possessors (ADP) background checks fit into projections. (0/10 IND, 1/3 MIL, 1/2 GA)

- Create a policy to increase organization accountability for keeping PRs up-to-date. One such incentive would be to mandate that anyone without an up-to-date PR (or at least a PR requested in a timely manner.) be removed from his or her position. Of course, this would require more expeditious investigations. (0/10 IND, 1/3 MIL, 0/2 GA)

- In the future, use JPAS as a management tool to track compliance with policy requirements. (0/10 IND, 1/3 MIL, 0/2 GA)

- Apply an across-the-board formula to contracts so that contractors could be held accountable for PSI requirements for cleared personnel. (0/10 IND, 1/3 MIL, 0/2 GA)

Increase Budget and Resources for Projections

A single respondent mentioned that there was a need for centralized funding for additional resources to improve the accuracy of the PSI data gathered and maintained by Security programs (0/10 IND, 1/3 MIL, 0/2 GA).

Recent Initiatives

Two new initiatives, one by the Army and one by the Air Force, are underway at the present time to improve projection of PSI requirements. The Army is developing a Total Army Personnel Security Investigations Management System (TAPSIMS). TAPSIMS will count and categorize incoming personnel security requests so that individual Army commanders will have a record of all requests submitted for enlisted personnel and officers in their command. This also will improve the quality of data aggregated across subcommands and, in turn, improve the data aggregated from the field for the total Army by Headquarters (Department of the Army, DCS for Intelligence) which is responsible for developing the Army's PSI projections.

The second initiative, undertaken by Headquarters, Air Force, is employing a "Systems Thinking" approach to model the flow of personnel through the Air Force system in an attempt to predict and control the number of background security investigations for the budget year plus two. The objective of this effort is to gain insight on how service policies, attrition, and assignment turnover interact and affect each other to generate requirements for security investigations. Initially, subject matter experts will map the policies and activities that generate the need for background investigations and will build a model covering the active Air Force (military officer, enlisted, and civilian). This model will provide officials with estimates of the number of investigations required as systems variables change. In the second phase of this effort, the active Air Force model will be modified to incorporate unique requirements of the Air Force Reserve and Air National Guard.

Both the Army and the Air Force efforts are consistent with the respondents' recommendations to develop a projection model that can be adapted by different organizations to project PSI requirements. Both studies should be completed in 2002.

Other Comments

A number of industry respondents expressed concern about the current backlog of investigations, which places a huge burden on industry (5/10 IND, 0/3 MIL, 0/2 GA). Delayed investigations cost industry large amounts of money as well as time because they often have to hire more than one individual to ensure that a cleared position can be filled once the investigations are completed. They also noted that their projections would be easier to develop and much more accurate once investigations are completed in a timely fashion and the CCMS is fully on board. On a positive note, they greatly appreciated DSS's responsiveness in cases where already cleared personnel are hired.

Appendix C

Development of a Personnel Security Clearance Adjudication Decision Support System for the Department of Defense (Executive Summary)

Development of a Personnel Security Clearance Adjudication Decision Support System for the Department of Defense:

Executive Summary

Purpose

The purpose of the overall project was to develop a plan for a Decision Support System (DSS) to assist adjudicators in making personnel security clearance eligibility determinations. As the name suggests, this Adjudication Decision Support (ADS) system is designed to support the adjudicators, not replace them. The ADS system will leverage expertise in the Central Adjudication Facilities (CAFs), acting as an expert force multiplier.

Phase I of this project, covered by this report, had four objectives: (1) review the adjudication decision process and identify the best type of DSS for an ADS system, (2) review the data elements in the Case Control Management System (CCMS) and the Joint Personnel Adjudication System (JPAS) and identify candidates for potential inclusion in the ADS system, (3) review commercial DSSs to determine those that could be employed, and (4) create an ADS system development plan.

Approach

The approach was multifaceted, designed to meet the four study objectives. The adjudication process was reviewed to identify the most promising type(s) of DSS. The CCMS and JPAS data dictionaries were reviewed to identify data elements offering promise. Descriptions of many commercial DSS tools and successful implementations were reviewed to determine the best approach for developing an ADS system. The information reviewed to address the first three objectives formed the basis for creating the ADS system development plan.

Findings

Three candidate DSS approaches were identified: (1) Rule-Based Reasoning (RBR), (2) Case-Based Reasoning (CBR), and (3) Artificial Neural Networks (ANN). Each approach has important advantages and some weaknesses. A hybrid system involving all three approaches is synergistic, as it can capitalize on the strengths of the individual approaches, while reducing their individual weaknesses.

Conclusions

The information reviewed for Phase I of this project supports the concept of an ADS system designed to assist adjudicators. If resources permit, the recommended custom-designed system would be contractor-developed, perhaps in part utilizing existing commercial products. Alternatively, if fewer resources are available, an in-house effort could be initiated on a smaller scale. An ADS system offers the promise of significant benefits for improving personnel security clearance processing. Adjudication decisions would be made in a more objective fashion, be more consistent and fair, and should be accomplished in less time, thereby addressing the current backlog problem, reducing costs, enhancing productivity, and improving customer satisfaction. Although a tool focused on assisting adjudicators can help alleviate only part of the entire personnel security clearance problem, the benefits to the entire system should be significant. The development plan described in this report can serve as the foundation for the next phase of this important personnel security research program.

Appendix D

Development of a Computerized Simulation Model of the Personnel Security Clearance Process for the Department of Defense: A Feasibility Study (Executive Summary)

Development of a Computerized Simulation Model of the Personnel Security Clearance Process for the Department of Defense: A Feasibility Study

Executive Summary

Background

Safeguarding classified information is an essential component of our national security system. This classified information covers a wide array of topics, ranging from strategic defense plans to state-of-the-art weapons systems to identification information on U.S and allied intelligence agents. Ensuring that the military, civilian, and contractor personnel in the Department of Defense (DoD) who have access to this classified information are loyal, trustworthy, and reliable is a central component of the security program.

The magnitude of the challenge is substantial. Approximately 200,000 personnel security clearance eligibility decisions are made each year for DoD Components alone. Other agencies outside of DoD that have a large number of positions requiring access to classified information (e.g., the National Security Agency, the Central Intelligence Agency, and the Department of Energy) significantly increase the total number of security clearance applications processed each year.

The accurate and timely processing of applications for personnel security clearances is critical to the DoD mission. The clearance process involves collecting background information on an applicant and evaluating the information obtained (both positive and negative) against thirteen standard adjudicative criteria. Serious current and longstanding problems involving large case backlogs have prompted numerous investigations over the past two decades. Attempted solutions have been piecemeal and, at best, only partially effective.

Purpose

The purpose of this study was to determine the feasibility and utility of developing a computerized model of the personnel security clearance processing system. Decision makers in the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD(C3I)) are the primary intended model users. In addition, the model will have potential value to decision makers in other DoD Components and to other agencies outside of DoD responsible for ensuring that these clearance decisions are made accurately and in a timely fashion.

Approach

Information was reviewed from sources on mathematical modeling of business procedures from management science, operations research, systems analysis, and computer simulation. The advantages and disadvantages of alternative procedures for modeling the clearance process were examined. These alternatives included general-purpose simulation tools, a spreadsheet approach, and the use of a computer programming language to construct the model. Both simulation languages and general-purpose computer programming languages were considered. Two primary candidate approaches were identified and levels of effort estimates were provided for the model. System performance criteria and example questions for model solution were presented. Key system, organization, and case variables were identified. Finally, the current personnel security clearance processes for DoD military, civilian, and contractor personnel were flowcharted and described.

Findings and Conclusions

Development of the model is feasible and offers the promise of providing a powerful and flexible decision support tool not only to ASD(C3I) decision makers, but also to other DoD agencies (e.g., the Defense Security Service) and government agencies outside of DoD (e.g., the Office of Personnel Management). The model would be useful to managers responsible for planning, policy, operations, evaluation, and costs of personnel security clearances. Some example uses of the model are:

- Simulating changes to the current personnel security processing system (e.g., alternative resource investment scenarios)

- Examining the predicted consequences of implementing alternative policies, both in terms of case backlogs and costs

- Evaluating the tradeoffs between competing strategies in terms of benefits and costs

- Identifying those strategies that offer the greatest net benefits

The model will provide decision makers with a powerful, flexible tool that can help address any personnel security clearance processing backlog problems and facilitate smooth operation of the clearance system in the future.

Appendix E

March 2002 Letter from the Aerospace Industries Association: Industrial Security “Fee-For-Service”

Industrial Security "Fee-For-Service" (08Mar02)

Issue:

The Director of the Defense Security Service (DSS) recently informed the Aerospace Industries Association (AIA) and National Defense Industrial Association (NDIA)[18] that the DOD Comptroller has indicated the intention to apply a "Fee-for-Service" (FFS) billing process for industrial security. Under this concept, cleared industrial facilities will be charged for the security activities of the DSS relative to its security "support" of those facilities. This process has been under consideration by DOD for several years and, as described, would be applied to military services and government civilian agency "customers" of the DSS as well as to cleared industrial facilities.

Background:

In concept, FFS seeks to impose a business-like discipline on those entities that request personnel security clearances (PCL) from the DSS   It assumes that if a monetary charge is established for having a BI completed and a PCL adjudicated (or other DSS service provided) the requesters will be more prudent in what they request and will only pursue essential security clearances and the fees received might then fund operations and create business equilibrium for the DSS. [19]

Aerospace Industries Association opposes application of this concept to Industry because DSS' legal relationship with cleared Industry makes FFS inappropriate for application to Industry. The DSS relationship with industry is *legally different* from its relationship with the military services and other government agencies it supports. This essential difference makes FFS inappropriate for application to Industry.

Discussion:

The DSS engages in two distinct activities with respect to cleared industrial facilities: It processes BIs leading to PCLs for contractor employees and it conducts security oversight of the cleared contractor's security system. The DSS pursues these two activities with respect to Industry under the long-standing legal mechanism of a "Department of Defense Security Agreement" (DD Form 441).

Section I (C) of the Security Agreement states:

> **"The Government** agrees, on written application**, to grant personnel security clearances to eligible employees of the Contractor who** require access **to information classified TOP SECRET, SECRET, or CONFIDENTIAL." [Emphasis added.]**

[18] Lt. Gen. Charles Cunningham spoke before a joint meeting of the AIA and NDIA Industrial Security Committees on 23 October at St. Petersburg, FL. The status of Fee-for-Service was one of many topics of interest that he addressed before this group of security professionals.

[19] It is well to note in passing that there has never been evidence produced to support any allegation that cleared contractors, individually or as a group, are requesting unnecessary PCLs.

It is clear from this language that the Government is legally obligated to provide security clearances for contractor employees upon the request of the contractor. Balancing that, the Government has an inherent right under the language of Sections I (C) and II of the Security Agreement to judge the actual need for a candidate employee to access classified information and require a PCL. That subjective assessment capability provides the Government with all the control mechanism it needs to prevent excessive requests for *contractor* clearances. No market mechanism and no monetary fee, is needed to control *assumed* excessive demand with respect to cleared contractors. If the two conditions of eligibility and need exist, then the Government (DOD and DSS) is obliged to provide, gratis to the contractor, the means to perform on classified contracts in the form of cleared employees. It is a security task that the Government denies the contractor the right to perform for itself. It is a *quid pro quo* for the contractor having assumed all the other costs of maintaining a compliant industrial security program.

Further, Section II of the Security Agreement, "Security Reviews," states in part:

> *"Designated representatives of the Government responsible for reviews pertaining to industrial plant security shall have the right to review, at reasonable intervals, the procedures, methods, and facilities utilized by the Contractor in complying with the requirements of the terms and conditions of the Manual…."*

It is evident from this wording that the Government has a right and an obligation to ensure that contractors comply with requirements of the National Industrial Security Program Operating Manual (NISPOM), to include requesting PCLs for only those employees who actually require access to classified information. It may inspect within reason and it may, as authorized by the NISPOM, approve or disapprove security systems that a contractor proposes to apply in specific cases. DSS may provide peripheral advice and assistance to a contractor during such approval transactions. *However, there is no "demand" from contractors for this DSS "service."* It is an oversight responsibility that the Government has, properly, placed upon itself. It is improper to propose charging a contractor for inspecting his facility or approving an information system to process classified data or examining a secure area to ensure that its construction meets the physical security standards of the NISPOM. Those are due diligence tasks the Government has set for itself, not to satisfy any contractor's wishes and desires, but rather to validate that Government information in the contractor's possession is being protected to established standards. It is thus neither logical nor contractually appropriate to suggest billing a contractor for the DSS oversight effort.

The only reference to monetary issues in the Security Agreement is found in Section VI, quoted as follows in its entirety:

> *Section VI - SECURITY COSTS*
> *This Agreement does not obligate Government funds, and the Government shall not be liable for any costs or claims of the Contractor arising out of this Agreement or instructions issued hereunder. It is recognized, however, that the parties may provide in other written contracts for security costs, which may be properly chargeable thereto.*

The terminology used has historically been interpreted as such, that the Government is hereby protecting *itself* against cleared contractors charging it for performing NISPOM-driven security tasks. The cost of industrial security to a cleared contractor is booked as overhead, except as specific classified contracts may be negotiated to levy security tasks above and beyond established NISPOM requirements. There is no provision in the Security Agreement or the NISPOM for the Government to charge cleared contractors for carrying out the security tasks and obligations that it has specifically reserved to itself. Further, under the current language of Section VI, there is no mechanism available, other than overhead allocation, for contractors to bill back the proposed FFS charges.

The security baseline for a program is established in the Contract Security Specification, identified as either a DD Form 254 or NF4.4702. It is prepared by the system acquisition agency, provided to the contractor, and provides the contractor with contractual direction related to programmatic classification guidance, security program requirements and identification of the cognizant security authority. All proposed security costs are based upon the security requirements contained in the Request for Proposal, including the initial Contract Security Specification, and are included in the overall contract value. Upon contract award, the contractor is contractually obligated to perform to the cost, schedule, and performance requirements (including security requirements) that have been negotiated and agreed upon. Any changes to the baseline established at contract award, including changes to security requirements are considered a change to the contract and are subject to equitable adjustment in the contract value. A monetary increase to an existing contract value will be based upon many factors, including government-mandated costs that were not proposed as part of the original contract.

The Fee-For-Service concept is a proposed contract modification and would be handled as a Class 1 change to an existing contract, in that the contractor is now being asked to support an activity that is out of scope of the original contract, and therefore subject to equitable adjustment of the cost, schedule, and performance requirements of the contract. A Class 1 change can have significant impact to contract cost; in this case security costs, associated with a specific program. Furthermore, this concept is an attempt by the DSS to unilaterally change the manner in which government security requirements are implemented on programs, without any obvious coordination with the various acquisition agencies. If FFS were implemented, all costs associated with this out of scope change would be passed on to the acquisition agency, not directly to DSS, resulting in an increased cost to our national programs.

Recommendation:

In the event that DSS must institute fee-for-service, Industry requests that an equitable, allowable and reasonableness test to government charges, be applied. Although DSS might have a monopoly on industry in this area, such a test would allow for cost controls for industry and the government would receive a substantial benefit from the fees. The revenue generated as a result of fees, could be used to improve the clearance process by hiring additional processors and implementing a new efficiently working system. In lieu of a monopoly by DSS, industry might expect a process that would allow utilization of an existing DoD sanctioned contract investigative agency whose cost, efficiency, quality of product and timeliness of delivery exceeded the benchmark of DSS.

Industry therefore opposes the concept of Fee-for-Service being applied to cleared contractors, both for security clearance processing and for industrial security oversight.

Appendix F

List of Acronyms

List of Acronyms

AAAP	Accelerated Access Authorization Program
AJ	Administrative Law Judge
ACES	Automated Continuing Evaluation System
ADSS	Adjudicative Decision Support System
AIA	Aerospace Industries Association
ANACI	Access National Agency Check with Inquiries
APSOC	Acting Personnel Security Oversight Committee
ASD	Assistant Secretary of Defense
C3I	Command, Control, Communications and Intelligence,
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAF	Central Adjudication Facilities
CCMS	Case Control Management System
CFR	Code of Federal Regulations
CHRI	Criminal History Record Information
CIA	Central Intelligence Agency
CIFA	Counterintelligence Field Activity
CIO	Chief Information Officer
CMB	Configuration Management Board
CRO	Central Requirements Office
DASD(S&IO)	Deputy Assistant Secretary of Defense for Security and Information Operations
DCI	Director of Central Intelligence
DCII	Defense Clearance and Investigations Index
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DIS	Defense Investigative Service
DISCO	Defense Industrial Security Clearance Office
DITTO	Defense Investigations Technology and Tracking Office
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDIG	Inspector General, DoD
DoDSI	Department of Defense Security Institute
DOE	Department of Energy
DOHA	Defense Office of Hearings and Appeals
DOJ	Department of Justice
DSS	Defense Security Service
EAP	Employee Assistance Programs
ENTNAC	Entrance National Agency Check
EO	Executive Order
EPSQ	Electronic Personnel Security Questionnaire
EQIP	Electronic Questionnaire for Investigation Processing
FBI	Federal Bureau of Investigation
FFS	Fee For Service
FSO	Facility Security Officer

GAO	General Accounting Office
GBSG	Government Business Services Group
IC	Intelligence Community
IPS	Independent Planning Study
IPT	Integrated Process Team
IT	Information Technology
JCS	Joint Chiefs of Staff
JPAS	Joint Personnel Adjudication System
JSC	Joint Security Commission
LAC	Local Agency Check
LI	Limited Inquiry
MAISAP	Major Automated Information Systems Acquisition Program
MAISARC	Major Automated Information Systems Acquisition Review Council
MSM	MSM Security Services
NAC	National Agency Check
NACI	National Agency Check with Inquiry
NACLC	National Agency Check with Local Agency Check and Credit Check
NRO	National Reconnaissance Office
NSA	National Security Agency
OASD(C3I)	Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence
OIPT	Overarching Integrated Process Team
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSD	Office of the Secretary of Defense
PBD	Program Budget Decision
PERSEREC	Defense Personnel Security Research Center
PIC	Personnel Investigations Center
PIPs	Personnel Investigation Processes
PL	Public Law
PMO	Program Management Office
POC	Point of Contact
PPBS	Planning Programming and Budgeting System
PR	Periodic Reinvestigations
PRT	Process Review Team
PSOC	Personnel Security Oversight Committee
PSAB	Personnel Security Appeal Board
PSI	Personnel Security Investigation
PSQ	Personnel Security Questionnaire
RAMP	Requirements and Adjudication Management Program
RFA	Reports for Adjudication
ROI	Report of Investigation
S&IO	Security and Information Operations
SAF	Secretary of the Air Force
SAF/AA	Administrative Assistant to the SAF
SAF/FM	Office of the Assist. Secretary of the Air Force (Financial Management Comptroller)

SAP	Special Access Programs
SCI	Sensitive Compartmented Information
SES	Senior Executive Service
SecDef	Secretary of Defense
SF-86	Standard Form 86 National Security Questionnaire
SII	Special Investigative Inquiry
SIOP-ESI	Single Integrated Operational Plan-Extremely Sensitive Information
SOW	Statement of Work
SSBI	Single Scope Background Investigation
TS	Top Secret
TS/SCI	Top Secret/ Sensitive Compartmented Information
USC	United States Code
USIS	US Investigations Services, Inc
WHS	Washington Headquarters Service
XML	Extensible Markup Language